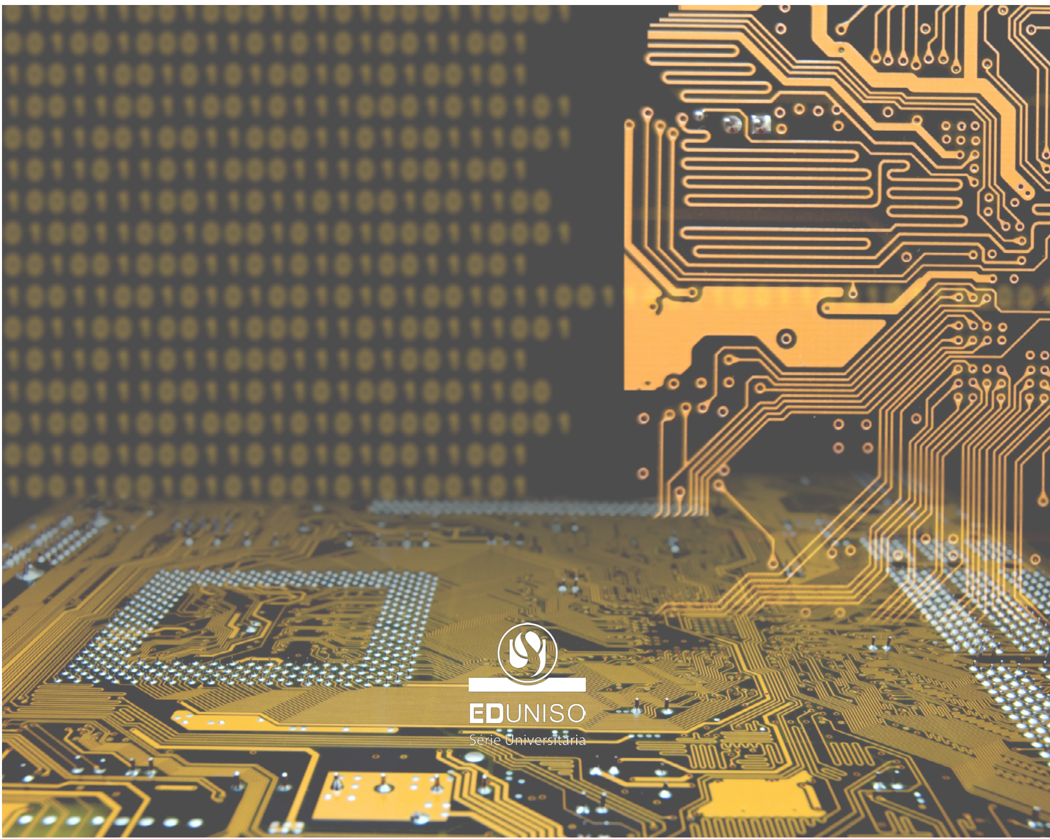
Augusto de Abreu Pires

FUNDAMENTOS MATEMÁTICOS PARA COMPUTAÇÃO

lógica e álgebra



EDUNISO: Editora da Universidade de Sorocaba
Rodovia Raposo Tavares, KM 92,5
18023-000 Vila Artura
Sorocaba / SP – Brasil
Fone: 15 – 2101 7018
E-mail: edunisoeditorauniso@gmail.com
http://uniso.br/eduniso/

Augusto de Abreu Pires

FUNDAMENTOS MATEMÁTICOS PARA COMPUTAÇÃO

lógica e álgebra

Sorocaba/SP
Eduniso
2017

Fundamentos matemáticos para computação: lógica e álgebra
Disponível também em formato impresso

Ficha Técnica
Normalização: Vilma Franzoni
Ilustração de capa: bagotaj/depositphotos
Projeto gráfico, Diagramação e Capa: Entrelinhas Editorial
Revisão: Lucas A. Giavoni
Secretaria: Silmara Pereira da Silva Martins

Ficha Catalográfica

Pires, Augusto de Abreu
P743f Fundamentos matemáticos para computação : lógica e álgebra / Augusto de Abreu Pires. – Sorocaba, SP : Eduniso, 2017.
232p.

ISBN: 978-85-61289-38-6
Obra financiada pela Uniso, através do Edital de Publicações 2016.

1. Lógica matemática. 2. Álgebra superior. I. Título.

CDD: 511.3

Elaborada por: Vilma Franzoni (CRB-8/4485)

DEDICATÓRIA

À minha esposa, Simone, e aos meus pais, Joaquim e Aracy, pela compreensão na minha ausência e pela paciência na minha presença…

PREFÁCIO

Esta obra trata de dois fundamentos da Ciência da Computação: A Lógica Matemática e a Álgebra Superior. Ambas suportam o desenvolvimento da Computação das últimas décadas e se tornam, assim, obrigatórias à perfeita compreensão dos conteúdos específicos dessa ciência e a pesquisa acadêmica nessa área.

Ao estudar a Lógica Matemática, além do Cálculo Proposicional e do Cálculo de Quantificadores, estudamos também as regras de raciocínio.

A Teoria dos Conjuntos decorre como consequência natural da Lógica Matemática, em particular do Cálculo Proposicional e do Cálculo de Quantificadores, e por isso também é tratada nesta obra.

Como opção ao processo de simplificação de fórmulas do Cálculo Proposicional, realizado em um primeiro momento pela aplicação de equivalências lógicas, apresentamos os Diagramas de Karnaugh, que sistematizam este processo.

Ao tratar da Álgebra Superior, estudamos os monoides, grupos, anéis e corpos, ou de forma geral, as diversas estruturas algébricas, entre elas a álgebra Booleana, em particular, a álgebra mínima ou álgebra dos computadores, a famosa álgebra dos zeros e uns.

APRESENTAÇÃO

No primeiro capítulo deste livro apresentaremos o Cálculo Proposicional: Operações com função de verdade, árvore de decomposição de fórmulas, tabelas de verdade, tautologias, contradições e contingências, árvore de refutação, equivalência lógica e consequência lógica e parênteses. Este capítulo destina-se à familiarização com as operações lógicas, aqui chamadas de operações com função de verdade, ao estudo da veracidade de uma fórmula e a comparação entre fórmulas.

No segundo capítulo estudaremos inicialmente dois procedimentos, fundamentados no primeiro capítulo, denominados construção de fórmulas, tal que a partir do comportamento de uma fórmula podemos encontrar a sua expressão. Neste capítulo estudaremos também as formas normais de uma fórmula, conjuntiva e disjuntiva, conteúdo de grande importância na programação de computadores e no estudo de circuitos eletroeletrônicos, quando a essência é a modelagem de situações problema a partir do seu comportamento. Ressaltamos que uma fórmula deve, sempre que possível, ser simplificadas, para o que utilizamos primeiramente as equivalências lógicas estudadas no primeiro capítulo e posteriormente, finalizando este capítulo, estudaremos a simplificação através dos diagramas de Karnaugh, um procedimento gráfico embasado nas equivalências lógicas.

O terceiro capítulo se dedica ao estudo das regras do raciocínio. Estudaremos as Regras de Inferência ou Regras de Dedução, que nos permitem realizar demonstrações, ou seja, tirar conclusões a partir de certas suposições, neste momento no Cálculo Proposicional.

Ampliando a nossa capacidade de raciocínio, no quarto capítulo estudaremos o Cálculo de Quantificadores, quando começaremos a trabalhar com outros tipos de expressões, aquelas que nos dão ideia de quantidade, para as quais outras regras de raciocínio são necessárias além daquelas estudadas para o Cálculo Proposicional.

No quinto capítulo apresentaremos uma introdução à Teoria dos Conjuntos, quando o leitor perceberá que esta teoria já lhe é familiar, isto é, conhecimentos adquiridos no Cálculo Proposicional são retomados com uma nova linguagem.

No capítulo seis apresentaremos a Álgebra Superior e Álgebra Booleana, quando, mais uma vez, o leitor perceberá a sua já familiaridade a este último conteúdo, conforme ocorreu com a Teoria dos Conjuntos, mas para tanto, muitos conceitos da Álgebra Superior devem preceder a apresentação da Álgebra Booleana.

No final de cada capítulo são propostos exercícios que viabilizarão a apropriação dos conteúdos estudados, e para que isso aconteça de forma plena, esses exercícios estão apresentados na mesma sequência do desenvolvimento dos conteúdos. Assim, devem ser resolvidos paralelamente ao estudo dos conceitos apresentados.

Para os futuros Matemáticos, em particular para os apaixonados por Lógica Matemática, e em especial pelo cálculo com proposições, sugerimos a leitura do artigo “Uma axiomatização para o cálculo proposicional”, após a leitura deste livro.

Terminamos esta apresentação afirmando que, embora esta obra possa ser recomendada como bibliografia básica em algumas disciplinas dos cursos de Graduação aqui citados, o que aqui apresentaremos se fará presente em muitas outras disciplinas desses cursos, de forma direta ou indireta, e assim, nessas disciplinas ou até mesmo em estudos na Pós-Graduação, ocorrerá a tão desejada interdisciplinaridade com a Matemática.

Esperamos que a leitura seja agradável e os conteúdos de muito proveito.

SUMÁRIO

1

Introdução

Motivado pela escassez de edições recentes de obras que contemplem satisfatoriamente os conteúdos a apresentar, este livro é indicado a várias disciplinas dos cursos que fazem da computação seu meio ou seu fim, além das habilitações em Matemática.

Consideramos como eixo norteador desta obra os Exames Nacionais de Desempenho dos Estudantes de cursos da área das Ciências Exatas e as Diretrizes Curriculares Nacionais para os cursos de Graduação em Computação, que tratam dos cursos de Bacharelado em Ciência da Computação, em Engenharia de Computação, em Engenharia de Software e em Sistemas de Informação.

Essas diretrizes, quanto aos conteúdos curriculares de formação básica, indicam a matemática do contínuo (cálculo, álgebra linear, equações diferenciais, geometria analítica, matemática aplicada - séries, transformadas e cálculo numérico), para a qual muitas obras recentemente editadas foram dedicadas, além de teoria dos grafos, probabilidade e estatística e pesquisa operacional e otimização, cujo estudo deve ser antecedido por conceitos da matemática do contínuo e para os quais também muitas obras foram recentemente editadas.

Além desses, essas mesmas diretrizes indicam a Análise Combinatória e a Matemática Discreta, também contemplados em publicações recentes. Estudaremos a Lógica Matemática e as Estruturas Algébricas, também indicadas nessas diretrizes, para os quais infelizmente temos poucas publicações recentes.

A escolha desses dois conteúdos se deve, além do motivo acima apresentado, pela analogia existente entre a Lógica Matemática e a Álgebra Booleana, uma estrutura algébrica fundamental à computação eletrônica. Também por esse motivo apresentaremos a Teoria dos Conjuntos, conteúdo indispensável no estudo de conceitos específicos da Ciência da Computação, como de Banco de Dados. Esses conteúdos, como todos os demais da área da Matemática, podem ser estudados sob diferentes níveis de complexidade, e assim nos utilizamos dos Exames Nacionais de Desempenho dos Estudantes para realizar a dosimetria na abordagem presente nesta obra.

Embora idealizada tendo como eixo norteador os programas dos cursos de Graduação já citados, esta obra pode ser útil também a alunos de alguns cursos do Ensino Médio Técnico. De fato, conhecimentos básicos sobre Lógica Matemática são indispensáveis a todos, pois dela fazem parte as regras do raciocínio, a quais, mesmo em situações cotidianas, são muitas vezes aplicadas de forma incorreta.

Convivemos com as famosas placas “não jogue lixo e entulho neste local”. Observem que é solicitado não jogar lixo E entulho, ou seja, é proibido descartar esses dois materiais no local. Mas descartar apenas um deles, de acordo com a placa, seria permitido. O correto é escrever “não jogue lixo e não jogue entulho” ou “não jogue lixo ou entulho”. Existem quatro possibilidades para o descarte de lixo e de entulho em um determinado local:

1: jogar lixo e jogar entulho;
2: jogar lixo e não jogar entulho;
3: não jogar lixo e jogar entulho;
4: não jogar lixo e não jogar entulho.

O que se deseja com a colocação da famosa placa é a quarta possibilidade, mas ela proíbe apenas a prática da primeira. A placa, portanto, permite o descarte de apenas um desses materiais, o que não é desejado. Por outro lado, jogar lixo ou entulho cobre as três primeiras possibilidades e, portanto, quando se proíbe jogar lixo ou entulho expressa-se o que de fato se deseja.

Outra expressão que muitas vezes não apresenta o que de fato se deseja impor é “não entre sem terno e gravata”. Ela tem a mesma estrutura da expressão do exemplo anterior, e portanto, não proíbe a entrada de uma pessoa que não usa terno, desde que ela esteja com gravata, como também não proíbe a entrada de uma pessoa sem gravata, desde que ela esteja trajando terno. A grafia correta é “não entre sem terno ou gravata”. O mesmo acontece no rótulo de alguns produtos, os quais embora de excelente qualidade, pecam na redação ao apresentar a informação “sem adição de açúcares e conservantes”.

Nos três exemplos mencionados, embora a grafia esteja incorreta, normalmente o recado é compreendido. Em outras situações, porém, a conclusão a que chegamos está equivocada. Como é verdade que, se alguém entra na piscina, então se molha, muitos concluem que se não entrar na piscina, então ficará seco. Ou ainda, estando molhado, conclui-se que entrou na piscina. No entanto, estas duas conclusões podem não ser verdadeiras, pois podemos nos molhar de outras formas, como por exemplo, em uma ducha.

As situações aqui descritas, quando mal compreendidas, podem, no máximo, provocar pequenas discussões, mas a troca de “e” por “ou”, ou vice-versa, na prática de programadores, de cientistas ou de engenheiros pode provocar desastres ou prejuízos. Por isso o estudo das regras do raciocínio na Lógica Matemática, tanto no Cálculo Proposicional como no Cálculo de Quantificadores, viabilizarão a correta compreensão do enunciado dos mais diversos problemas profissionais ou acadêmicos, além de compreender e concluir corretamente em situações simples como as anteriormente apresentadas.

Atualmente, sem exceção, de todas as áreas emergem problemas cuja solução exige a parceria da Computação. No entanto, a modelagem destes podem nos conduzir a situações complexas, e então a simplificação destas colaborará para a desejada eficiência. Para tanto, é essencial a devida fundamentação teórica, pois sem ela, por exemplo, é possível programar, mas não é possível estudar a sua eficiência, a diferença essencial entre um programador e um bom programador.

Assim, este texto foi elaborado para os estudantes e docentes que não se contentam apenas com as aplicações, considerando essencial a fundamentação teórica para a completa compreensão e apropriação do conteúdo. Aos nossos leitores, porém, pedimos paciência, pois a aplicação de muitos conteúdos estudados neste livro ocorrerá em outros momentos da vida acadêmica ou mesmo na profissional dos que agora nos dão o prazer da leitura.

Encerrando esta introdução, esclarecemos que nesta obra não nos preocuparemos com contextualizações, e desta forma o nosso estudo se realizará através de fórmulas, sem nos preocuparmos com o significado delas. Assim, conforme o que neste texto estudaremos, um raciocínio do tipo “se eu for ao baile então serei aprovado em Lógica Matemática e como fui ao baile posso concluir que serei aprovado em Lógica Matemática” é matematicamente válido, correto, no entanto bem sabemos que ir ao baile não tem a ver com a aprovação nessa disciplina. Na verdade, a Lógica Matemática não pode de fato preocupar-se com as contextualizações, pois, se também esse fosse seu objeto de estudo, como ela é aplicada em raciocínios que permeiam todas as Ciências, o estudante da Lógica Matemática deveria ser conhecedor de todas as Ciências.

2

Cálculo proposicional

2.1 Os operandos do Cálculo Proposicional

Definição: Chamamos de *valor verdade* os estados de qualquer situação bi-estável.

Exemplo: Quente e frio, aceso e apagado, verdadeiro e falso, entre outros.

Trabalharemos sempre com os valores verdade *verdadeiro*, geralmente indicado por V ou por 1, e *falso*, geralmente indicado por F ou por 0, salvo menção contrária.

Definição: *Proposição* (no Cálculo Proposicional) é toda expressão sobre a qual faz sentido estabelecer o seu valor verdade, ou seja, é qualquer expressão na qual se tenha sentido afirmar se seu conteúdo é verdadeiro ou falso.

Exemplo: São proposições:

"A neve é branca"

"3 é um número par"

"$4 > 5$"

"$2 > 1$".

Não serão consideradas proposições expressões do tipo:

"Amanhã vai chover"

"Os Estados Unidos ganharão a guerra contra o terrorismo"
"Vou ser aprovado em Lógica".

Para representar uma proposição, usaremos as letras minúsculas p, q, r, acompanhadas ou não de índices inferiores que pertençam ao conjunto dos números inteiros não negativos (Z_+).

Exemplo: Dada a proposição "2 é menor que 3", podemos representá-la por p, ou p_0 (lê-se p zero), ou p_1 (lê-se p um), ou mais genericamente, por qualquer p ou q ou r ou ainda por p_i ou q_i ou r_i em que $i \in Z_+$.

Notação: p: 2 é menor que 3 significará p representando a proposição "2 é menor que 3", e a notação é análoga para outras representações.

Definição: Se p é uma proposição que assume o valor verdade verdadeiro, dizemos que o *valor lógico* da proposição p é verdadeiro, o que indicamos por vl(p) = V. Analogamente, se p é uma proposição que assume o valor verdade falso, dizemos que o *valor lógico* da proposição p é falso, o que indicamos por vl(p) = F. É importante observar que dada uma certa proposição, ela assume um dos dois valores, verdadeiro (V), ou falso (F), nunca ambos simultaneamente, e não existe um terceiro valor.

2.1.1 Operações com função de verdade

Definição: Dizemos que uma *operação* é com *função de verdade* se o valor lógico (verdadeiro ou falso) da proposição resultante é determinado pelos valores lógicos das proposições a partir das quais esta foi construída.

2.1.1.1 Operação negação

É uma operação unitária, isto é, que opera uma proposição e fornece como resultado uma segunda proposição. É o exemplo mais simples de uma operação com função de verdade. Se p é uma proposição, indicaremos a negação de p por - p, ou por ~ p, ou ainda por p'.

Exemplo: Se p representa a proposição "a neve é branca", denotamos por:

p: a neve é branca.

Daí - p representa a proposição "a neve não é branca", e denotamos:

- p: a neve não é branca.

Note que se vl(p) = V, então vl(- p) = F, e se vl(p) = F, então vl(- p) = V.

Podemos descrever uma tabela que resuma como se comporta a operação com função de verdade chamada *negação*. Para tanto seja p uma proposição qualquer:

p	- p
V	F
F	V

A tabela acima nos diz que se vl(p) = V, então vl(- p) = F, e que se vl(p) = F, então vl(- p) = V.

Observe ainda que vl(- - p) = vl(p).

2.1.1.2 Operação conjunção

É uma operação binária, isto é, que opera duas proposições e fornece como resultado uma terceira proposição. Essa operação com função de verdade, chamada *conjunção*, evidencia o uso da palavra "e" na linguagem usual e será denotada pelo símbolo $\wedge$, ou $\cdot$, ou ainda &. Assim, se p e q são duas proposições, diremos que $p \wedge q$ representa a conjunção de p com q, e lê-se p e q.

É fácil se convencer de que o valor lógico da proposição $p \wedge q$ é verdadeiro somente quando ambos os valores lógicos de p e de q forem também verdadeiros. Assim analisaremos o valor lógico de $p \wedge q$ de acordo com os valores verdade (V ou F) que são atribuídos a p e q, conforme a tabela abaixo:

p	q	$p \wedge q$
V	V	V
V	F	F
F	V	F
F	F	F

Note que só quando vl(p) = vl(q) = V, temos vl($p \wedge q$) = V, nos demais casos vl($p \wedge q$) = F.

Na conjunção p ∧ q, p e q recebem o nome de *conjuntivos*.

2.1.1.3 Operação disjunção

Essa operação com função de verdade é representada pelo uso da palavra “ou”.

Existem dois tipos de disjunção:

Operação disjunção inclusiva: Essa operação com função de verdade, chamada *disjunção inclusiva*, representa o uso da palavra “ou” e será representada pelo símbolo ∨, ou +. Sejam, p representando a proposição “João é muito esperto” e q representando a proposição “João é muito sortudo”. A utilização de “p ∨ q” resulta na proposição:

“João é muito esperto ou João é muito sortudo”.

Nesta frase vemos que nada impede que João seja esperto e sortudo, isto é, não se exclui a possibilidade de João ser tanto esperto como sortudo, ou ainda podemos dizer que o uso de “p ou q” no sentido inclusivo faz com que a situação se prevaleça para p, ou para q, ou para ambos p e q.

Operação disjunção exclusiva: Essa operação com função de verdade, chamada *disjunção exclusiva*, também representa o uso da palavra “ou” e será representada pelo símbolo “x∨”. Sejam, p representando a proposição “João vai passar esta tarde no clube” e q representando a proposição “João vai estudar em casa esta tarde”. A utilização de “p x∨ q” resulta na proposição:

“João vai passar esta tarde no clube ou João vai estudar em casa esta tarde”.

É evidente que não se tem o caso em que João vai passar esta tarde no clube e João vai estudar em casa esta tarde, ao mesmo tempo. Isto é o que caracteriza o uso de “ou” no sentido exclusivo, isto é, vale para p, ou vale para q, mas não é válido para ambos.

Pelo exposto temos que p ∨ q representará “p ou q ou ambos” e sua tabela será dada por:

p	q	p ∨ q
V	V	V
V	F	V
F	V	V
F	F	F

Note que vl(p $\vee$ q) = F somente quando vl(p) = vl(q) = F. Nos demais casos vl(p $\vee$ q) = V.

Agora, p x$\vee$ q representará "somente p ou somente q" e sua tabela será dada por:

p	q	p x$\vee$ q
V	V	F
V	F	V
F	V	V
F	F	F

Note que vl(p x$\vee$ q) = F somente quando vl(p) = vl(q). Nos demais casos vl(p x$\vee$ q) = V.

Na disjunção (inclusiva e exclusiva), p e q são chamados de *disjuntivos*.

Quando cita-se simplesmente *disjunção*, devemos considerar a disjunção inclusiva.

2.1.1.4 Operação condicional

É muito comum em matemática usarmos a expressão "se $\cdots$ então $\cdots$", e aqui vamos então analisar o que acontece com a operação com função de verdade correspondente. Isto é, sendo p e q proposições, analisaremos o que acontece com "se p então q". Usaremos o símbolo $\rightarrow$ para representar esta operação, que recebe o nome de *condicional*, e daí "se p então q" será representado por p $\rightarrow$ q, em que p é chamado de *antecedente* da condicional e q de *consequente* da condicional.

Para facilitar a compreensão faremos a análise através de um exemplo. Sejam, p representando a proposição "João saiu na chuva" e q representando a proposição "João se molhou". A proposição resultante será:

"Se João saiu na chuva então João se molhou".

É evidente que se o antecedente da condicional for verdadeiro e o consequente da condicional for falso, a proposição toda será falsa. Voltando ao exemplo acima teríamos: "Se João saiu na chuva então João não se molhou" (esqueça a hipótese de João ter levado um guarda-chuva ou uma capa!), que é uma frase falsa. Observe que nos demais casos, a proposição resultante será verdadeira (quando João não sai na chuva ele pode se molhar por outro motivo!).

A tabela que representa a condicional é dada por:

p	q	$p \to q$
V	V	V
V	F	F
F	V	V
F	F	V

O $vl(p \to q) = F$ somente quando $vl(p) = V$ e $vl(q) = F$, nos demais casos $vl(p \to q) = V$.

Observe que a operação condicional não goza de comutatividade, isto é, $p \to q$ nem sempre produz o mesmo resultado que $q \to p$, ao contrário da conjunção, da disjunção inclusiva e da disjunção exclusiva.

Considerando uma instituição escolar na qual a média para aprovação é sete, outro exemplo para esta operação é "se o aluno foi aprovado então a média foi maior ou igual a sete". Com certeza o caso da aprovação ser verdadeira com média maior ou igual a 7 falso, contrariaria o regimento escolar, e o caso da aprovação ser falsa com média maior ou igual a 7 verdadeiro não é estranho, pois a aprovação não depende apenas da média. Observe neste exemplo que aprovação e média maior ou igual a sete não são situações equivalentes, na verdade a aprovação implica em média maior ou igual a sete, mas o contrário não é verdadeiro, ou seja, média maior ou igual a sete não implica na aprovação. Esse conceito de implicação será aprofundado com mais detalhes posteriormente.

Nos dois exemplos anteriores existe uma relação entre o antecedente da condicional e o consequente da condicional, mas isso nem sempre acontece. De agora em diante o símbolo $\to$ será usado para representar a implicação material, isto é, se preocupará unicamente com os valores verdade atribuídos, e não com a possível relação que exista entre o antecedente da condicional e o consequente da condicional.

Outras expressões, que também representam a operação condicional $p \to q$ na linguagem usual são:

Tendo-se p então q;
Quando p então q;
Sempre que p, q;
q sempre que se tenha p;
p é condição suficiente para q;
q é condição necessária para p;
q se p, entre outras.

2.1.1.5 Operação bicondicional

Em matemática, o uso da bicondicional é evidenciado pela expressão "$\cdots$ se e somente se $\cdots$". A operação com função de verdade correspondente, chamada *bicondicional*, será por nós representada pelo símbolo $\leftrightarrow$, ou seja, "p se e somente se q" será representada por $p \leftrightarrow q$.

Sejam, p representando a proposição "o gelo derrete" e q representando a proposição "estar exposto a temperatura acima de 0º C". Neste caso $p \leftrightarrow q$ torna-se:

"O gelo derrete se e somente se está exposto a temperatura acima de 0º C".

Convenhamos que seria muito estranho se tivéssemos que o gelo está derretendo e, ao checarmos a temperatura, verificássemos que é falso que ela está acima de 0º C ou ainda, se com a falsidade da temperatura acima de 0º C verificássemos que o gelo derrete, concordando com a tabela da operação bicondicional:

p	q	$p \leftrightarrow q$
V	V	V
V	F	F
F	V	F
F	F	V

Como se observa $vl(p \leftrightarrow q) = V$ sempre que $vl(p) = vl(q)$.

O que deve ser observado é que temos dois caminhos que devem ser satisfeitos, a saber:

Da esquerda para a direita ($\rightarrow$):

"Se o gelo derrete então está exposto a temperatura acima de 0º C", ($p \rightarrow q$).

Da direita para a esquerda ($\leftarrow$):

"Se está exposto a temperatura acima de 0º C então o gelo derrete", ($q \rightarrow p$).

A conjunção desses dois caminhos caracteriza a bicondicional. Portanto $p \leftrightarrow q$ representa "$p \rightarrow q$ e $q \rightarrow p$", ou seja, $p \leftrightarrow q$ é o mesmo que $(p \rightarrow q) \wedge (q \rightarrow p)$.

Assim, em vez de apresentarmos a tabela dessa operação, como fizemos anteriormente, podemos construir a sua tabela:

Coluna 1	Coluna 2	Coluna 3	Coluna 4	Coluna 5
p	q	$(p \rightarrow q)$	$(q \rightarrow p)$	$(p \rightarrow q) \wedge (q \rightarrow p)$
V	V	V	V	V
V	F	F	V	F
F	V	V	F	F
F	F	V	V	V

Vamos explicar a construção desta tabela.

As colunas 1 e 2 foram formadas analisando-se todas as possibilidades existentes de se atribuir os valores V e F simultaneamente a p e q. A coluna 3 foi obtida aplicando-se a tabela da operação condicional às colunas 1 e 2, nesta ordem. A coluna 4 foi obtida aplicando-se a tabela da operação condicional às colunas 2 e 1, nesta ordem. Finalmente, obtivemos a coluna 5 aplicando-se a tabela da operação conjunção às colunas 3 e 4.

Outras expressões, que também representam a operação bicondicional $p \leftrightarrow q$ na linguagem usual são:

p se e só se q;

p equivale a q;

p é condição necessária e suficiente para q, entre outras.

Até aqui, introduzimos 6 operações com funções de verdade e as representamos por símbolos:

$$-, \wedge, \vee, x\vee, \rightarrow \text{ e } \leftrightarrow.$$

Para facilitar a linguagem, esses símbolos serão chamados de *conectivos*.

Quando temos apenas uma proposição, digamos p, sabemos que ela pode possuir o valor lógico verdadeiro ou falso, e assim uma tabela para uma única proposição possui apenas duas linhas de valores verdade:

p
V
F

Agora, quando temos duas proposições, digamos p e q, existem quatro possibilidades diferentes de atribuirmos os valores verdade verdadeiro ou falso a estas duas proposições, simultaneamente consideradas. Assim, uma tabela para duas proposições possui quatro linhas de valores lógicos:

p	q
V	V
V	F
F	V
F	F

Nada, porém, impede que uma proposição seja constituída por várias proposições distintas. Então quantas possibilidades diferentes existem de atribuirmos os valores verdade verdadeiro ou falso simultaneamente à n proposições?

Observe que para uma proposição existem duas possibilidades distintas ($2 = 2^1$) e para duas proposições existem quatro possibilidades diferentes ($4 = 2^2$).

Uma regra pode ser deduzida disso: para n proposições, teremos 2^n linhas.

Quando n = 3, isto é, para três proposições, digamos p, q e r, temos 2^3 possibilidades apresentadas na seguinte tabela:

p	q	r
V	V	V
V	V	F
V	F	V
V	F	F
F	F	F
F	F	V
F	V	F
F	V	V

Para a construção destas oito possibilidades tomamos as primeiras quatro linhas, ou seja, a metade do total, e atribuímos o valor verdade verdadeiro à primeira proposição, no caso p e em seguida construímos as quatro possibilidades diferentes de atribuirmos os valores lógicos verdadeiro ou falso às outras proposições, no caso p e q, simultaneamente consideradas. Finalizando, copiamos as quatro primeiras linhas já construídas para as outras quatro linhas da tabela, substituindo V por F e F por V. Esta mesma regra pode ser utilizada para um número maior de proposições.

Outras regras existem para esta mesma finalidade, como por exemplo, preencher a primeira coluna colocando na primeira metade das 2^n linhas o valor verdade V e na segunda metade o valor verdade F, e depois repetindo o procedimento nas demais colunas alternando a colocação de V e F em quantidades iguais a metade das quantidades de V ou F utilizados na coluna anterior, até preencher a última coluna, alternando um V e um F. Nesta metodologia, com n = 3, isto é, para três proposições, digamos p, q e r, temos a seguinte tabela:

p	q	r
V	V	V
V	V	F
V	F	V

V	F	F
F	V	V
F	V	F
F	F	V
F	F	F

Neste livro adotamos a primeira metodologia apresentada.

Na Matemática, quando denotamos um número por uma letra, digamos x, esta letra recebe o nome de variável. Da mesma forma, no Cálculo Proposicional as proposições, representadas pelas letras minúsculas p, q, r, acompanhadas ou não de índices inferiores que pertençam ao conjunto dos números inteiros não negativos (Z_+), serão chamadas de *variáveis proposicionais (v. p.)*.

Nosso próximo passo é saber identificar, sem ambiguidade, expressões construídas com o uso dos conectivos. Por exemplo, na expressão $p \vee q \wedge r$, sendo vl(p) = V, vl(q) = V e vl(r) = F, podemos ter que vl($p \vee q \wedge r$) = V ou vl($p \vee q \wedge r$) = F, dependendo de qual operação com função de verdade executamos primeiro. Para resolvermos este problema, vamos introduzir o conceito de fórmula.

Definição: Definimos como *fórmula bem formada (fbf),* ou simplesmente fórmula, qualquer expressão construída com variáveis proposicionais pela aplicação de um número finito de conectivos, satisfazendo:

1) Toda variável proposicional sozinha é fórmula;

2) Se A e B são fórmulas, então - A, $(A \wedge B)$, $(A \vee B)$, $(A \, x\!\vee B)$, $(A \rightarrow B)$, $(A \leftrightarrow B)$ também são fórmulas;

3) Somente são fórmulas as expressões que são determinadas por meio das condições 1 e 2.

As fórmulas serão denotadas por letras maiúsculas do alfabeto, acompanhadas ou não de índices inferiores que pertençam ao conjunto dos números inteiros não negativos (Z_+).

Observações:

1) - A não é necessariamente uma fórmula. - A será uma fórmula sempre que A o for. Isto é - A é uma fórmula somente se especificarmos que A é uma fórmula.

2) $(A \wedge B)$, $(A \vee B)$, $(A\ x\!\vee B)$, $(A \rightarrow B)$ ou $(A \leftrightarrow B)$ não são necessariamente fórmulas. $(A \wedge B)$, $(A \vee B)$, $(A\ x\!\vee B)$, $(A \rightarrow B)$ ou $(A \leftrightarrow B)$ só serão fórmulas se especificarmos que A e B são fórmulas.

3) As tabelas das operações com função de verdade, negação (-), conjunção ($\wedge$), disjunção ($\vee$ ou $x\!\vee$), condicional ($\rightarrow$), e bicondicional ($\leftrightarrow$), são ainda válidas se substituirmos as proposições p e q por fórmulas A e B quaisquer.

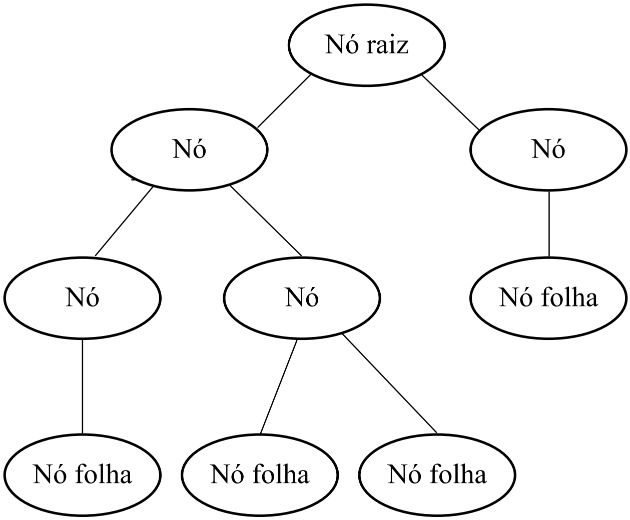
Exemplo: Segundo as condições enunciadas p, - p, r_{23}, $(p \vee q)$, - $(p \wedge q)$, $(r_{23} \rightarrow p)$, $((r_{23}\ x\!\vee p) \leftrightarrow (p \vee q))$, são consideradas fórmulas, mas r_{23}, $p \vee q$, $r_{23} \rightarrow p$, $(r_{23} \rightarrow p) \leftrightarrow (p \vee q)$, - $p \wedge q$, $s \vee q$, A, $(B \vee C)$ não são consideradas fórmulas.

Definição: A última operação que realizamos em uma fórmula determina o seu tipo. Assim, sendo A e B fórmulas quaisquer, temos cinco tipos de fórmula:

- Negação: as fórmulas do tipo - A;
- Conjunção: as fórmulas do tipo $(A \wedge B)$;
- Disjunção: as fórmulas do tipo $(A \vee B)$ ou do tipo $(A\ x\!\vee B)$;
- Condicional: as fórmulas do tipo $(A \rightarrow B)$; e
- Bicondicional: as fórmulas do tipo $(A \leftrightarrow B)$.

2.2 Árvore de decomposição

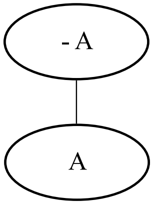
É um processo gráfico, tal que dada uma fórmula A, no qual determinam-se todas as fórmulas que a compõem. Estas fórmulas componentes recebem o nome de *subfórmulas* da fórmula A. Como no Cálculo Proposicional, temos uma operação unitária e as demais binárias. A árvore de decomposição de uma fórmula é uma árvore binária, isto é, na qual cada ramificação se divide em no máximo duas novas ramificações. Uma árvore binária qualquer é apresentada a seguir, apenas para familiarização.



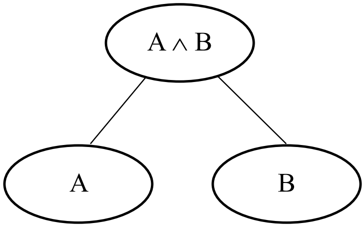
No caso de árvores de decomposição de fórmulas do Cálculo Proposicional, o nó raiz é composto pela fórmula a ser decomposta, e os demais nós por suas subfórmulas. Quando a decomposição a ser realizada se refere a uma operação binária (conjunção, disjunção, condicional ou bicondicional) entre duas subfórmulas, então o nó é decomposto em dois outros nós. E quando a decomposição a ser realizada se refere a operação negação, que é unitária, então o nó é decomposto em um único outro nó. A árvore de decomposição está completa somente quando obtemos os nós folhas, que no caso de fórmulas do Cálculo Proposicional, são as variáveis proposicionais, que também são consideradas subfórmulas.

Assim, se A e B são fórmulas, temos as seguintes decomposições possíveis:

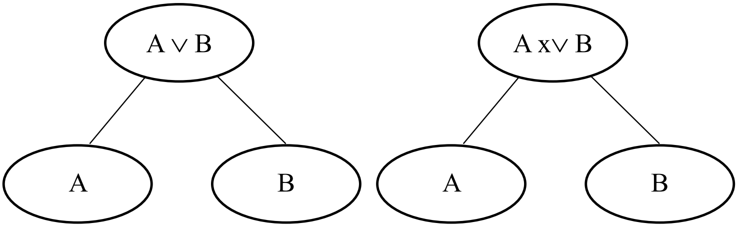
- Decomposição de uma negação:



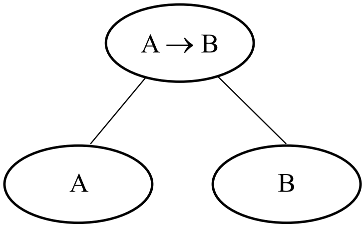
- Decomposição de uma conjunção:



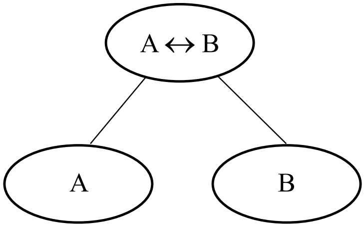
- Decomposição de uma disjunção:



- Decomposição de uma condicional:



- Decomposição de uma bicondicional:

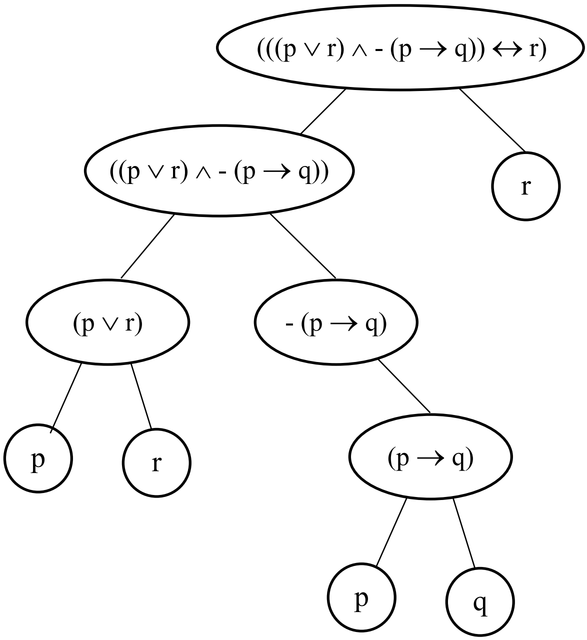


As decomposições propostas estão terminadas somente se as fórmulas A e B forem variáveis proposicionais, caso contrário devem ser continuadas.

Exemplo: Construir a árvore de decomposição da fórmula

$$(((p \vee r) \wedge - (p \rightarrow q)) \leftrightarrow r),$$

e determinar todas as suas subfórmulas:



As subfórmulas da fórmula $(((p \vee r) \wedge - (p \rightarrow q)) \leftrightarrow r)$ são: p, q, r, $(p \rightarrow q)$, $(p \vee r)$, $- (p \rightarrow q)$, $((p \vee r) \wedge - (p \rightarrow q))$, e a própria $(((p \vee r) \wedge - (p \rightarrow q)) \leftrightarrow r)$.

2.3 Tabela de verdade

Podemos dizer que toda fórmula A define uma *função de verdade*. Isto é, para cada atribuição de valores verdade feita às variáveis proposicionais de A, podemos calcular o valor lógico correspondente a fórmula A. Este cálculo pode ser exposto por meio de uma tabela chamada *tabela de verdade*.

Para se construir a tabela de verdade de uma fórmula A qualquer, devemos seguir os seguintes passos:

1º passo: Construa a árvore de decomposição da fórmula A e determine todas as suas subfórmulas;

2º passo: Escreva na primeira linha da tabela todas as subfórmulas de A, começando com as variáveis proposicionais e, em seguida, as demais subfórmulas, sendo que a última será a própria fórmula A, obedecendo a regra de que uma subfórmula é colocada nesta primeira linha da tabela somente depois que todas as suas subfórmulas já foram colocadas;

3º passo: Complete as colunas das variáveis proposicionais com todas as possibilidades distintas de atribuirmos os valores lógicos verdadeiro (V) e falso (F) simultaneamente à estas variáveis, lembrando que se temos n variáveis proposicionais existem 2^n atribuições distintas;

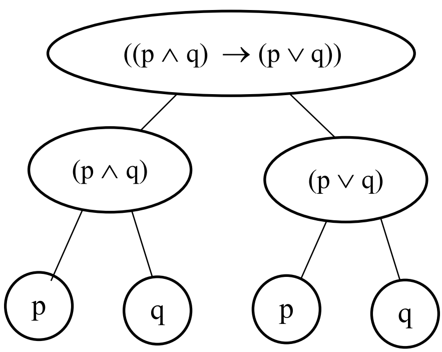
4º passo: Complete as demais colunas, na sequência em que você escreveu as subfórmulas, usando as tabelas das operações com função de verdade.

Vamos agora ver em alguns exemplos como se constrói tal tabela.

Exemplo: Seja A a fórmula:

$$((p \wedge q) \rightarrow (p \vee q)).$$

Sua árvore de decomposição é:



Suas subfórmulas são: p, q, $(p \wedge q)$, $(p \vee q)$ e $((p \wedge q) \rightarrow (p \vee q))$.

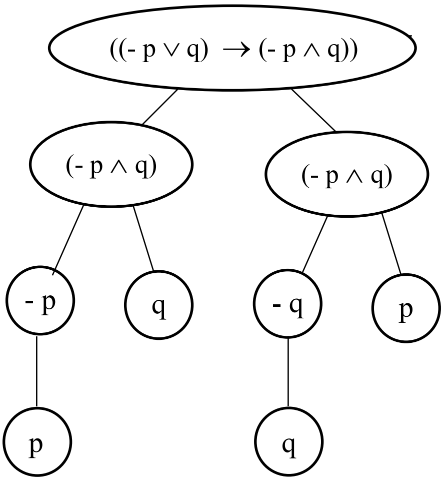
Sua tabela de verdade é:

p	q	$(p \wedge q)$	$(p \vee q)$	$((p \wedge q) \rightarrow (p \vee q))$
V	V	V	V	V
V	F	F	V	V
F	V	F	V	V
F	F	F	F	V

Exemplo: Construa a tabela de verdade para a fórmula:

$$((- p \vee q) \rightarrow (- q \wedge p)).$$

Sua árvore de decomposição é:



Suas subfórmulas são: p, q, $- p$, $- q$, $(- p \vee q)$, $(- q \wedge p)$ e $((- p \vee q) \rightarrow (- q \wedge p))$.

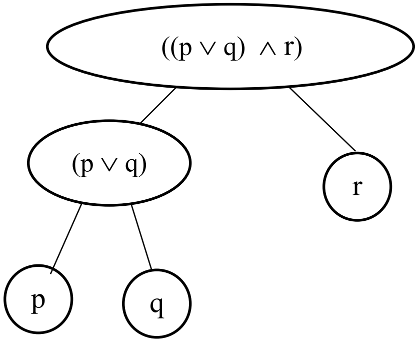
Sua tabela de verdade é:

p	q	$- p$	$- q$	$(- p \vee q)$	$(- q \wedge p)$	$((- p \vee q) \rightarrow (- q \wedge p))$
V	V	F	F	V	F	F
V	F	F	V	F	V	V
F	V	V	F	V	F	F
F	F	V	V	V	F	F

Exemplo: Construa a tabela de verdade para a fórmula:

$((p \vee q) \wedge r)$.

Sua árvore de decomposição é:



Suas subfórmulas são: p, q, r, $(p \vee q)$ e $((p \vee q) \wedge r)$.
Sua tabela de verdade é:

p	q	r	$(p \vee q)$	$((p \vee q) \wedge r)$
V	V	V	V	V
V	V	F	V	F
V	F	V	V	V
V	F	F	V	F
F	F	F	F	F
F	F	V	F	F
F	V	F	V	F
F	V	V	V	V

2.4 Tautologia, contradição e contingência

Definição: Dizemos que uma fórmula A é *tautologia* se ela assume o valor lógico verdadeiro (V) para todas as atribuições de valores verdade feitas às suas variáveis proposicionais.

Notação: Se A é uma fórmula e A é uma tautologia, indicaremos por $\vdash$ A.

A partir deste ponto não mais construiremos a árvore de decomposição, apenas determinaremos as subfórmulas a serem listadas na primeira linha da tabela de verdade. Aconselhamos ao leitor que continue a construir essa árvore, até que na determinação das subfórmulas esteja completamente seguro.

Exemplo: Seja A a fórmula:

$$(p \vee - p).$$

Suas subfórmulas são: p, - p e $(p \vee - p)$.

Sua tabela de verdade é:

p	- p	$(p \vee - p)$
V	F	**V**
F	V	**V**

Logo, $\vdash$ A, isto é, A é uma tautologia.

Observe que se B é uma fórmula qualquer então toda fórmula do tipo $(B \vee - B)$ é uma tautologia.

Exemplo: Seja C a fórmula:

$$- ((p \vee q) \wedge (- p \wedge - q)).$$

Suas subfórmulas são: p, q, - p, - q, $(p \vee q)$, $(- p \wedge - q)$, $((p \vee q) \wedge (- p \wedge - q))$ e $- ((p \vee q) \wedge (- p \wedge - q))$.

Sua tabela de verdade é:

p	q	- p	- q	$(p \vee q)$	$(- p \wedge - q)$	$((p \vee q) \wedge (- p \wedge - q))$	$- ((p \vee q) \wedge (- p \wedge - q))$
V	V	F	F	V	F	F	**V**
V	F	F	V	V	F	F	**V**
F	V	V	F	V	F	F	**V**
F	F	V	V	F	V	F	**V**

Logo, $\vdash$ C, isto é, C é uma tautologia.

Definição: Dizemos que uma fórmula A é uma *contradição* se ela assume o valor lógico falso (F) para todas as atribuições de valores verdade feitas às suas variáveis proposicionais.

Exemplo: Seja A a fórmula:

$$(p \wedge - p).$$

Suas subfórmulas são: p, $-p$ e $(p \wedge -p)$.

Sua tabela de verdade é:

p	- p	(p ∧ - p)
V	F	**F**
F	V	**F**

Logo, a fórmula A é uma contradição.

Observe que, se B é uma fórmula qualquer, então toda fórmula do tipo $(B \wedge -B)$ é uma contradição.

Exemplo: Seja C a fórmula:

$$-((p \vee q) \vee (-p \wedge -q)).$$

Suas subfórmulas são: p, q, $-p$, $-q$, $(p \vee q)$, $(-p \wedge -q)$, $((p \vee q) \vee (-p \wedge -q))$ e $-((p \vee q) \vee (-p \wedge -q))$.

Sua tabela de verdade é:

p	q	- p	- q	(p ∨ q)	(- p ∧ - q)	((p ∨ q) ∨ (- p ∧ - q))	- ((p ∨ q) ∨ (- p ∧ - q))
V	V	F	F	V	F	V	**F**
V	F	F	V	V	F	V	**F**
F	V	V	F	V	F	V	**F**
F	F	V	V	F	V	V	**F**

Logo, a fórmula C é uma contradição.

Definição: As fórmulas que não são contradições, nem tautologias, são chamadas *contingências*.

Exemplo: Seja A a fórmula:

$$((p \rightarrow q) \wedge (q \rightarrow p)).$$

Suas subfórmulas são: p, q, $(p \rightarrow q)$, $(q \rightarrow p)$ e $((p \rightarrow q) \wedge (q \rightarrow p))$.

Sua tabela de verdade é:

p	q	(p → q)	(q → p)	((p → q) ∧ (q → p))
V	V	V	V	**V**
V	F	F	V	**F**
F	V	V	F	**F**
F	F	V	V	**V**

Logo, a fórmula A é uma contingência.

2.5 Árvore de refutação

A árvore de refutação[1] é outro procedimento utilizado para analisar o *valor veritativo* de fórmulas, isto é, analisar se uma fórmula é uma tautologia, contradição ou contingência, uma vez que a construção da tabela de verdade pode tornar-se inviável, principalmente quando a fórmula a analisar possui um número elevado de variáveis proposicionais.

Para a sua construção da árvore de refutação de uma fórmula qualquer A, siga os seguintes passos:

1º passo: Construa a árvore de decomposição da fórmula A e determine todas as suas subfórmulas;

2º passo: Escreva na primeira linha da tabela todas as subfórmulas de A, começando com as variáveis proposicionais, e em seguida as demais subfórmulas, sendo que a última será a própria fórmula A. Obedeça a regra de que uma subfórmula é colocada nesta primeira linha da tabela somente depois que todas as suas subfórmulas já tenham sido colocadas;

3º passo: Atribua o valor lógico falso (F) à fórmula A, se você pretende demonstrar que A é uma tautologia, ou atribua o valor lógico verdadeiro (V) à fórmula A se você pretende demonstrar que A é uma contradição (observe que você está supondo um absurdo!);

4º passo: Da direita para a esquerda, analise cada uma das subfórmulas de A a partir do absurdo suposto inicialmente (dependendo dos conectivos que compõem a fórmula A, pode ser necessário o estudo de mais de um caso para certas subfórmulas de A);

Se você detectar um absurdo, ou seja, uma variável proposicional com os valores-lógico verdadeiro e falso simultaneamente, em decorrência do absurdo suposto inicialmente, está concluída a demonstração (caso tenha sido necessário o estudo de mais de um caso para certas subfórmulas de A, este absurdo deve ser obtido em todos os casos). Quando tal absurdo não for encontrado, conclui-se apenas que a fórmula dada não é uma tautologia

1 Mais sobre árvore de refutação pode ser consultado no livro *Introdução à lógica para a ciência da computação*, de J. Minoro Abe, Alexandre Scalzitti e J. Inácio Silva Filho.

se a sua suposição inicial foi que ela assumia o valor lógico F, e conclui-se apenas que a fórmula dada não é uma contradição se a sua suposição inicial foi que ela assumia o valor lógico V.

É conveniente escrever uma última coluna na sua tabela, na qual você deve escrever as justificativas de cada conclusão obtida a partir do absurdo suposto inicialmente.

Observamos que no primeiro passo, conforme já comentamos, não construiremos a árvore de decomposição.

Exemplo: Seja A a fórmula:

$$((p \wedge q) \rightarrow q)).$$

Vamos verificar se A é uma tautologia.

Suas subfórmulas são: p, q, $(p \wedge q)$ e $((p \wedge q) \rightarrow q))$.

Sua árvore de refutação é:

p	q	$(p \wedge q)$	$((p \wedge q) \rightarrow q))$	Justificativa
			F	Absurdo suposto
	F	V		Tabela da operação condicional
V	**V**			Tabela da operação conjunção

Observe que obtemos um absurdo. A variável proposicional q deve assumir simultaneamente os valores lógicos verdadeiro e falso para que o valor lógico da fórmula $((p \wedge q) \rightarrow q))$ seja falso.

Logo a fórmula $((p \wedge q) \rightarrow q))$ é uma tautologia.

Exemplo: Seja B a fórmula:

$$((p \vee q) \wedge (- p \wedge - q)).$$

Vamos verificar se B é uma contradição.

Suas subfórmulas são: p, q, - p, - q, $(p \vee q)$, $(- p \wedge - q)$ e $((p \vee q) \wedge (- p \wedge - q))$.

Sua árvore de refutação é:

p	q	- p	- q	$(p \vee q)$	$(- p \wedge - q)$	$((p \vee q) \wedge (- p \wedge - q))$	Justificativa
						V	Absurdo suposto
				V	V		Tabela da operação conjunção

		V	V				Tabela da operação conjunção
F	**F**						Tabela da operação negação
				V			Transcrição da segunda linha
V	**V**						Tabela da operação disjunção inclusiva
V	F						Tabela da operação disjunção inclusiva
F	**V**						Tabela da operação disjunção inclusiva

Observe que temos $vl(p \vee q) = V$ em três casos distintos:

$$vl(p) = V \text{ e } vl(q) = V,$$
$$vl(p) = V \text{ e } vl(q) = F,$$
$$vl(p) = F \text{ e } vl(q) = V.$$

Em todos temos que os valores verdade em negrito se contradizem com os valores verdade, também em negrito, obtidos acima.

Logo, a fórmula $((p \vee q) \wedge (- p \wedge - q))$ é uma contradição.

Observação: Quando uma fórmula A possui conectivo(s) que exige(m) que mais de uma caso seja(m) analisado(s), é possível detectar que se trata de uma contingência se o absurdo ocorrer somente para alguns casos e não nos demais.

2.6 Equivalência lógica e consequência lógica

Definição: Dizemos que as fórmulas A e B são *logicamente equivalentes* se e somente se A e B sempre tomam o mesmo valor lógico para qualquer atribuição de valores verdade feita às variáveis proposicionais de A e B. Isto é, a última coluna das tabelas de verdade de A e de B são, necessariamente, as mesmas.

Notação: Se A e B são duas fórmulas logicamente equivalentes, indicaremos por A eq B ou $A \Leftrightarrow B$.

Exemplo: Seja A a fórmula:

$$- (p \vee q),$$

e seja B a fórmula:

$$(- p \wedge - q).$$

As subfórmulas da fórmula $-(p \vee q)$ são: p, q, $(p \vee q)$ e $-(p \vee q)$.

As subfórmulas da fórmula $(-p \wedge -q)$ são: p, q, $-p$ $-q$ e $(-p \wedge -q)$.

Daí as respectivas tabelas de verdade são:

p	q	$(p \vee q)$	$-(p \vee q)$	$-p$	$-q$	$(-p \wedge -q)$
V	V	V	**F**	F	F	**F**
V	F	V	**F**	F	V	**F**
F	V	V	**F**	V	F	**F**
F	F	F	**V**	V	V	**V**

Logo A eq B, isto é, as fórmulas A e B são logicamente equivalentes.

Observe que utilizamos a mesma atribuição de valores verdades para p e q na construção das tabelas de verdade de ambas as fórmulas.

Algumas equivalências lógicas se destacam pela grande utilização, principalmente na simplificação de expressões, e por isto recebem o nome de e*quivalências notáveis*:

1) Dupla Negação – DN:

$$- - A \text{ eq } A$$

2) Leis Idempotentes – LI:

$$\text{i) } (A \vee A) \text{ eq } A$$
$$\text{ii) } (A \wedge A) \text{ eq } A$$

3) Leis Comutativas – CL:

$$\text{i) } (A \vee B) \text{ eq } (B \vee A)$$
$$\text{ii) } (A \wedge B) \text{ eq } (B \wedge A)$$

4) Leis Associativas – AL:

$$\text{i) } ((A \vee B) \vee C) \text{ eq } (A \vee (B \vee C))$$
$$\text{ii) } ((A \wedge B) \wedge C) \text{ eq } (A \wedge (B \wedge C))$$

5) Leis de De Morgan – DL:

$$\text{i) } -(A \vee B) \text{ eq } (-A \wedge -B)$$
$$\text{ii) } -(A \wedge B) \text{ eq } (-A \vee -B)$$

6) Leis Distributivas – LD:

$$\text{i) } (A \vee (B \wedge C)) \text{ eq } ((A \vee B) \wedge (A \vee C))$$
$$\text{ii) } (A \wedge (B \vee C)) \text{ eq } ((A \wedge B) \vee (A \wedge C))$$

7) Leis Condicionais – LC:

$$(A \to B) \text{ eq } (- B \to - A)$$
$$(A \to B) \text{ eq } (- A \vee B)$$

8) Leis Bicondicionais – LB:

$$(A \leftrightarrow B) \text{ eq } ((A \to B) \wedge (B \to A))$$
$$(A \leftrightarrow B) \text{ eq } - (A \, x\vee \, B)$$

9) Elementos Neutros – EN:

$$A \vee F \text{ eq } A$$
$$A \wedge V \text{ eq } A$$

10) Elementos Complementares – EC:

$$A \vee - A \text{ eq } V$$
$$A \wedge - A \text{ eq } F$$

A, B, e C são fórmulas quaisquer e V e F são tautologias e contradições, respectivamente.

Definição: Dizemos que uma fórmula A *implica logicamente* uma fórmula B se e somente se para cada atribuição de valores verdade, feita às variáveis proposicionais de A e B, tal que o valor lógico de A é verdadeiro (V), temos o valor lógico de B também verdadeiro (V). Dizemos também que B é *consequência lógica* de A.

Notação: Se A e B são duas fórmulas e A implica logicamente B (ou B é consequência lógica de A), indicaremos por $A \vdash B$ ou $A \Rightarrow B$.

Exemplo: Seja A a fórmula:

$$(p \wedge q),$$

e seja B a fórmula:

$$(p \vee q).$$

As subfórmulas da fórmula $(p \wedge q)$ são: p, q e $(p \wedge q)$.

As subfórmulas da fórmula $(p \vee q)$ são: p, q, e $(p \vee q)$.

Daí as respectivas tabelas de verdade são:

p	q	$(p \wedge q)$	$(p \vee q)$
V	V	**V**	**V**
V	F	F	V
F	V	F	V
F	F	F	F

Logo, $(p \wedge q)$ implica logicamente $(p \vee q)$, ou o que é o mesmo $(p \vee q)$ é consequência lógica de $(p \wedge q)$.

Observe que $(p \vee q)$ não implica logicamente $(p \wedge q)$.

2.7 Alguns resultados sobre equivalência lógica, consequência lógica e tautologia

Teorema 1: Sejam A e B fórmulas. A eq B se e somente se $\models (A \leftrightarrow B)$, em outras palavras, A e B são logicamente equivalentes se e somente se $(A \leftrightarrow B)$ é uma tautologia.

Demonstração: Suponhamos primeiramente que $(A \leftrightarrow B)$ é uma tautologia (e então mostraremos que A eq B). Então $vl((A \leftrightarrow B)) = V$, isto é, independentemente dos valores verdade atribuídos às variáveis proposicionais em $(A \leftrightarrow B)$, o valor lógico da fórmula $(A \leftrightarrow B)$ é verdadeiro (V). Então, para cada atribuição particular de valores verdade para essas variáveis proposicionais, temos que $vl(A) = vl(B) = V$ ou $vl(A) = vl(B) = F$. Assim, A e B têm as mesmas colunas no final de suas tabelas de verdade, e portanto A eq B.

Suponhamos agora que as fórmulas A e B são logicamente equivalentes (e então mostraremos que $(A \leftrightarrow B)$ é uma tautologia). Consideremos qualquer atribuição de valores verdade feita às variáveis proposicionais de A e B. Se para uma certa atribuição o valor lógico de A é verdadeiro (V), então o valor lógico de B também é verdadeiro (V), pois estamos supondo A eq B. Analogamente, se para esta atribuição temos $vl(A) = F$, então, como A eq B, $vl(B) = F$. Assim, sempre teremos $vl((A \leftrightarrow B)) = V$, isto é, $(A \leftrightarrow B)$ é uma tautologia.

Teorema 2: Sejam A e B duas fórmulas, $A \models B$ se e somente se $\models (A \rightarrow B)$, em outras palavras, A implica logicamente B (ou B é consequência lógica de A) se e somente se $(A \rightarrow B)$ é uma tautologia.

Demonstração: Sabemos que a fórmula A implica logicamente a fórmula B se e somente se para cada atribuição de valores verdade, feita às variáveis proposicionais de A e B, tal que o valor lógico de A é verdadeiro (V), então o valor lógico de B também é verdadeiro (V). Ou seja, se e somente se nunca acontecer o caso em que o valor lógico de A é verdadeiro (V) e o valor lógico de B é falso (F), isto é, se e somente se $(A \to B)$ nunca é falso, ou seja, se e somente se $(A \to B)$ é uma tautologia.

Definição: Sejam $A_1, A_2, \cdots, A_n$ e B fórmulas. Dizemos que as $A_1, A_2, A_3 \cdots, A_n$ *implicam logicamente* B se e somente se para cada atribuição de valores verdade, feita às variáveis proposicionais de $A_1, A_2, \cdots, A_n$ e B, tal que o valor lógico de $A_1, A_2, \cdots, A_n$ são simultaneamente verdadeiros (V), temos que o valor lógico de B também é verdadeiro (V). Dizemos também que B é *consequência lógica* de $A_1, A_2, \cdots, A_n$.

Notação: Se $A_1, A_2, \cdots, A_n$ e B são fórmulas e $A_1, A_2, \cdots, A_n$ implicam logicamente B (ou B é consequência lógica de $A_1, A_2, \cdots, A_n$), indicaremos por $A_1, A_2, \cdots, A_n \vdash B$.

Teorema 3: Sejam $A_1, A_2, \cdots, A_n$ e B fórmulas. $A_1, A_2, \cdots, A_n \vdash B$ se e somente se $(\cdots (A_1 \wedge A_2) \wedge \cdots \wedge A_n) \vdash B$. Em outras palavras, $A_1, A_2, \cdots, A_n$ implicam logicamente B se e somente se $(\cdots (A_1 \wedge A_2) \wedge \cdots \wedge A_n)$ implica logicamente B.

Demonstração: Os valores lógicos de $A_1, A_2, \cdots, A_n$ são simultaneamente verdadeiros se e somente se o valor lógico de $(\cdots (A_1 \wedge A_2) \wedge \cdots \wedge A_n)$ é verdadeiro. Então $A_1, A_2, \cdots, A_n \vdash B$ se e somente se o valor lógico de B é verdadeiro sempre que o valor lógico de $(\cdots (A_1 \wedge A_2) \wedge \cdots \wedge A_n)$ é verdadeiro, isto é, $A_1, A_2, \cdots, A_n \vdash B$ se e somente se $(\cdots (A_1 \wedge A_2) \wedge \cdots \wedge A_n) \vdash B$.

Teorema 4: Sejam $A_1, A_2, \cdots, A_n$ e B fórmulas. $A_1, A_2, \cdots, A_n \vdash B$ se e somente se $\vdash ((\cdots (A_1 \wedge A_2) \wedge \cdots \wedge A_n) \to B)$, em outras palavras, $A_1, A_2, \cdots, A_n$ implicam logicamente B se e somente se $((\cdots (A_1 \wedge A_2) \wedge \cdots \wedge A_n) \to B)$ é uma tautologia.

Demonstração: No teorema 3 vimos que $A_1, A_2, \cdots, A_n \vdash B$ se e somente se $((\cdots (A_1 \wedge A_2) \wedge \cdots \wedge A_n) \vdash B$. Assim, pelo teorema 2, temos que $A_1, A_2, \cdots, A_n \vdash B$ se e somente se $\vdash ((\cdots (A_1 \wedge A_2) \wedge \cdots \wedge A_n) \to B)$.

Proposição 1: Sejam $A_1, A_2, \cdots, A_n$ e B fórmulas. Então vale a seguinte equivalência lógica:

$$(A_1 \to (A_2 \to (\cdots \to (A_n \to B)\cdots) \text{ eq } (\cdots((A_1 \wedge A_2) \wedge A_3) \wedge \cdots \wedge A_n) \to B).$$

Demonstração: O valor lógico de $(\cdots((A_1 \wedge A_2) \wedge A_3) \wedge \cdots \wedge A_n) \rightarrow B)$ é falso (F) se e somente se o valor lógico de $(\cdots((A_1 \wedge A_2) \wedge A_3) \wedge \cdots \wedge A_n)$ é verdadeiro (V) e o valor lógico de B é falso (F). Agora, o valor lógico de $(\cdots((A_1 \wedge A_2) \wedge A_3) \wedge \cdots \wedge A_n)$ é verdadeiro (V) se e somente se os valores lógicos de $A_1, A_2, \cdots, A_n$ são simultaneamente verdadeiros (V). Logo, o valor lógico de $(\cdots((A_1 \wedge A_2) \wedge A_3) \wedge \cdots \wedge A_n) \rightarrow B)$ é falso (F) se e somente se os valores lógicos de $A_1, A_2, \cdots, A_n$ são simultaneamente verdadeiros (V) e o valor lógico de B é falso (F).

Agora, o valor lógico de $(A_1 \rightarrow (A_2 \rightarrow (\cdots \rightarrow (A_n \rightarrow B)\cdots)$ é falso (F) se e somente se o valor lógico de A_1 é verdadeiro e o valor lógico de $(A_2 \rightarrow (\cdots \rightarrow (A_n \rightarrow B)\cdots)$ é falso (F). Isso equivale dizer que os valores lógicos de A_1 e A_2 são simultaneamente verdadeiros (V) e o valor lógico de $(A_3 \rightarrow (\cdots \rightarrow (A_n \rightarrow B)\cdots)$. Raciocinando analogamente, concluímos que o valor lógico de $(A_1 \rightarrow (A_2 \rightarrow (\cdots \rightarrow (A_n \rightarrow B)\cdots)$ é falso (F) se e somente se os valores lógicos de $A_1, A_2, \cdots, A_n$ são simultaneamente verdadeiros (V) e o valor lógico de B é falso (F).

Logo, $A_1 \rightarrow (A_2 \rightarrow (\cdots \rightarrow (A_n \rightarrow B)\cdots)$ eq $(\cdots((A_1 \wedge A_2) \wedge A_3) \wedge \cdots \wedge A_n) \rightarrow B)$.

Teorema 5: Sejam $A_1, A_2, \cdots, A_n$ e B fórmulas. $A_1, A_2, \cdots, A_n \vdash B$ se e somente se $\vdash (A_1 \rightarrow (A_2 \rightarrow (\cdots \rightarrow (A_n \rightarrow B)\cdots)$. Em outras palavras, $A_1, A_2, \cdots, A_n$ implicam logicamente B se e somente se $(A_1 \rightarrow (A_2 \rightarrow (\cdots \rightarrow (A_n \rightarrow B)\cdots)$ é uma tautologia.

Demonstração: Dos resultados anteriores, sabemos que $A_1, A_2, \cdots, A_n \vdash B$ se e somente se $(\cdots (A_1 \wedge A_2) \wedge \cdots \wedge A_n) \vdash B$, se e somente se $((\cdots (A_1 \wedge A_2) \wedge \cdots \wedge A_n) \rightarrow B)$ é uma tautologia. Pela proposição 1:

$(A_1 \rightarrow (A_2 \rightarrow (\cdots \rightarrow (A_n \rightarrow B)\cdots)$ eq $(\cdots((A_1 \wedge A_2) \wedge A_3) \wedge \cdots \wedge A_n) \rightarrow B)$

Disto, concluímos que $A_1, A_2, \cdots, A_n \vdash B$ se e somente se $\vdash (A_1 \rightarrow (A_2 \rightarrow (\cdots \rightarrow (A_n \rightarrow B)\cdots)$.

Corolário 1: Sejam $A_1, A_2, \cdots, A_n$ e B fórmulas. Se $A_1, A_2, \cdots, A_n \vdash B$ então $A_{i1}, A_{i2}, \cdots, A_{in} \vdash B$ onde $i_1, i_2, \cdots, i_n$ é qualquer permutação dos inteiros $1, 2, \cdots, n$.

Demonstração: Segue da equivalência notável, Lei Comutativa.

Vamos agora, apresentar alguns resultados gerais a respeito de tautologias.

Proposição 2: Sejam A e B fórmulas. Se A e $(A \rightarrow B)$ são tautologias, então B também é uma tautologia.

Demonstração: Suponhamos que vl(B) = F para alguma atribuição de valores verdade feita às variáveis proposicionais de A e B. Então, como A é uma tautologia, temos que vl(A) = V para todas as atribuições de valores verdade feita às variáveis proposicionais de A e B. Assim $(A \rightarrow B)$ terá o valor lógico falso (F) para alguma atribuição de valores verdade feita às variáveis proposicionais de A e B, contradizendo o fato de $(A \rightarrow B)$ ser tautologia. Portanto, B nunca terá o valor lógico falso (F). Logo, B também é uma tautologia.

Proposição 3: Sejam $A, A_1, A_2, \cdots, A_n$ e B fórmulas. Se A é uma tautologia contendo como variáveis proposicionais $p_1, p_2, \cdots, p_n$ e B resulta de A pela substituição das variáveis proposicionais $p_1, p_2, \cdots, p_n$ pelas fórmulas $A_1, A_2, \cdots, A_n$ respectivamente, então B é uma tautologia, isto é, substituição em uma tautologia produz uma tautologia.

Demonstração: Assumamos que A é uma tautologia. Para cada atribuição de valores verdade feita às variáveis proposicionais de B as fórmulas $A_1, A_2, \cdots, A_n$ terão valores lógicos $x_1, x_2, \cdots, x_n$, em que x_1, $1 \leq i \leq n$, é verdadeiro (V) ou falso (F).

Se nós assinalarmos $x_1, x_2, \cdots, x_n$ para $p_1, p_2, \cdots, p_n$ respectivamente, então o valor lógico resultante de A será o mesmo valor lógico de B. Como A é tautologia, seu valor lógico será sempre verdadeiro (V). Assim, B sempre toma o valor lógico verdadeiro (V), ou seja, B é uma tautologia.

Exemplo: Como a fórmula:

$$- ((p \vee q) \wedge (- p \wedge - q))$$

é uma tautologia, temos que para quaisquer fórmulas A e B a fórmula:

$$- ((A \vee B) \wedge (- A \wedge - B))$$

também é uma tautologia.

2.8 Parênteses

Existem fórmulas que levam um grande número de parênteses, tornando-se às vezes, difícil sua compreensão. Vamos então fazer algumas convenções para eliminar e recolocar parênteses de fórmulas de modo que estas não percam suas características. É necessário lembrar que um par de parênteses pode ser eliminado somente quando a sua recolocação reconduza à fórmula original, através dos critérios que seguem:

1) Os parênteses externos podem ser eliminados sem perdas, isto é, toda fórmula que não seja uma variável proposicional ou uma negação, leva um par de parênteses externos que pode ser omitido;

2) Para qualquer conectivo, adotaremos o princípio de associação à esquerda. Por exemplo, para restabelecer os parênteses na fórmula $p \vee q \vee r$, fazemos uma associação à esquerda, isto é, como primeiro passo a fórmula torna-se $(p \vee q) \vee r$, e em seguida, a próxima associação à esquerda, ou seja, como segundo passo a fórmula torna-se $((p \vee q) \vee r)$;

3) Adotaremos uma ordem hierárquica de força entre os conectivos. Os conectivos $-$, $\wedge$, $\vee$, $x\vee$, $\rightarrow$, $\leftrightarrow$, estão em ordem crescente de força, isto é, numa restauração de parênteses em uma fórmula, coloca-se parênteses primeiro nos mais fracos e assim sucessivamente até esgotar todos os conectivos. Para restaurar os parênteses na seguinte fórmula:

$$p \leftrightarrow - p_1 \vee p_2 \wedge p_3,$$

procedemos assim:

primeiro passo: $p \leftrightarrow - p_1 \vee (p_2 \wedge p_3)$;

segundo passo: $p \leftrightarrow (- p_1 \vee (p_2 \wedge p_3))$;

terceiro passo: $(p \leftrightarrow (- p_1 \vee (p_2 \wedge p_3)))$.

Observações:

1) Existem fórmulas que não podemos retirar todos os parênteses, pois sua omissão acarretará numa mudança de característica da fórmula. Por exemplo, na fórmula $- (p \vee q)$ não podemos retirar todos os parênteses, pois se o fizermos teremos a seguinte expressão $- p \vee q$. A partir desta última fórmula, se quisermos

restaurar os parênteses, de acordo com as convenções acima citadas, obteríamos $(- p \vee q)$ e esta fórmula é diferente da original.

O mesmo acontece com a fórmula $(p \to (p \to q))$. Retirando-se os parênteses segundo as convenções acima, obteríamos de maneira corretamente abreviada a fórmula $p \to (p \to q)$. Note que a fórmula $p \to p \to q$ não é uma simplificação correta, pois, recolocando-se os parênteses na fórmula $p \to p \to q$ obtemos $((p \to p) \to q)$, a qual não é logicamente equivalente a fórmula $(p \to (p \to q))$. Assim como estas, existem muitas fórmulas, nas quais não podemos eliminar todos os parênteses.

2) Já vimos que as fórmulas $((A \vee B) \vee C)$ e $(A \vee (B \vee C))$ são logicamente equivalentes. Eliminando-se o máximo possível de parênteses da fórmula $((A \vee B) \vee C)$ chegamos à expressão $A \vee B \vee C$, e assim o mesmo vale para $(A \vee (B \vee C))$, como também para a disjunção exclusiva e para a conjunção. Em outras palavras, podemos eliminar todos os parênteses das fórmulas $(A \vee (B \vee C))$, $(A \vee (B \vee C))$, $(A \text{ x}\vee (B \text{ x}\vee C))$, $(A \text{ x}\vee (B \text{ x}\vee C))$, $((A \wedge B) \wedge C)$ e $(A \wedge (B \wedge C))$.

3) Este tópico deverá ser considerado sempre que se fizer necessário.

2.9 Exercícios propostos

1) Sejam as proposições:

p: João é bom aluno;

q: João é estudioso.

i) Escreva na linguagem usual as seguintes sentenças:

a) $p \vee q$

b) $p \wedge q$

c) $p \text{ x}\vee - q$

d) $- p \wedge - q$

e) $- - p$

f) $p \to q$

g) $p \leftrightarrow q$

h) $- (- p \wedge - q)$

ii) Escreva na linguagem simbólica as seguintes sentenças:

a) João é bom aluno mas não é estudioso.

b) João é estudioso ou João é bom aluno.
c) Se João é bom aluno então João é estudioso.
d) Não é verdade que João é bom aluno e estudioso.
e) João é bom aluno se e só se é estudioso.
f) É falso que João não é estudioso.

2) Reescreva as sentenças seguintes procurando esclarecer o seu significado:
a) Não é verdade que João é bom aluno e estudioso.
b) É falso que João não é bom aluno e não é estudioso.
c) Não é verdade que João é bom aluno ou estudioso.
d) Não é verdade que João não é bom aluno ou é estudioso.
e) É falso que João não é estudioso.

3) Sabendo que vl(p) = V e vl(q) = F, determinar o valor lógico de cada uma das proposições:
a) $p \wedge - q$
b) $p \vee - q$
c) $- p \wedge q$
d) $- p \wedge - q$
e) $- p \, x\!\vee - q$
f) $p \wedge (- p \vee q)$
g) $- p \rightarrow q$
h) $- q \rightarrow p$
i) $- p \leftrightarrow q$

4) Determinar vl(p) em cada um dos seguintes casos, sabendo que:
a) $vl(q) = F$ e $vl(p \wedge q) = F$
b) $vl(q) = F$ e $vl(p \vee q) = F$
c) $vl(q) = F$ e $vl(p \rightarrow q) = F$
d) $vl(q) = F$ e $vl(p \rightarrow q) = V$
e) $vl(q) = V$ e $vl(p \leftrightarrow q) = F$
f) $vl(q) = F$ e $vl(p \leftrightarrow q) = V$

5) Determinar vl(p) e vl(q) em cada um dos seguintes casos, sabendo que:

a) vl($p \rightarrow q$) = V e vl($p \wedge q$) = F
b) vl($p \rightarrow q$) = V e vl(p x$\vee$ q) = F
c) vl($p \leftrightarrow q$) = V e vl($p \wedge q$) = V
d) vl($p \leftrightarrow q$) = F e vl($- p \vee q$) = V

6) Determinar os valores lógicos das proposições abaixo:

a) $p \wedge (- q \rightarrow (r \wedge p_0))$, sabendo que vl(p) = F
b) $(p \leftrightarrow q) \vee (q \rightarrow - p)$, sabendo que vl(q) = F
c) $(- p \vee r) \rightarrow (q \rightarrow p_0)$, sabendo que vl(q) = F
d) $((p \rightarrow q) \wedge p) \rightarrow - p$, sabendo que vl(p) = F
e) $(p \rightarrow r) \vee q$, sabendo que vl(r) = V

7) Escreva o antecedente e o consequente de cada uma das seguintes sentenças:

a) Se a chuva continuar então o rio vai transbordar.
b) Uma condição suficiente para a falha de uma rede elétrica é que a chave central desligue.
c) Os abacates estão maduros quando estão cremosos e macios.
d) Uma boa dieta é uma condição necessária para um gato ser saudável.

8) Classifique as fórmulas dadas abaixo como tautologia, contradição ou contingência:

a) $((p \vee q) \leftrightarrow (q \vee p))$
b) $((p \text{ x}\vee q) \wedge (- p \wedge - q))$
c) $(p \leftrightarrow (p \vee q))$
d) $(((p \rightarrow q) \wedge q) \rightarrow p)$
e) $((p \vee q) \rightarrow (- p \wedge - q))$
f) $(- p \rightarrow (p \text{ x}\vee q))$
g) $((p \text{ x}\vee q) \leftrightarrow (q \rightarrow p))$
h) $(p \leftrightarrow - p)$
i) $((p \wedge (q \vee r)) \leftrightarrow ((p \wedge q) \vee (p \wedge r)))$
j) $((p \rightarrow q) \rightarrow ((p \rightarrow r) \rightarrow (p \rightarrow r)))$
k) $(p \wedge - (p \text{ x}\vee q))$

l) $((p \veebar q) \rightarrow (- q \rightarrow p))$
m) $((p \rightarrow q) \leftrightarrow (- p \vee q))$
n) $((p \rightarrow q) \rightarrow (- q \rightarrow - p))$
o) $((p \rightarrow (q \veebar r)) \leftrightarrow ((p \wedge q) \vee (p \rightarrow r)))$
p) $((p \rightarrow q) \leftrightarrow - (p \wedge - q))$
q) $((p \wedge q) \rightarrow (- q \rightarrow - p))$
r) $((q \leftrightarrow (q \rightarrow p)) \rightarrow p)$

9) Através de árvore de refutação, verifique se as fórmulas abaixo são tautologias ou contradições:
a) $(p \leftrightarrow - p)$
b) $((p \rightarrow q) \rightarrow (- q \rightarrow - p))$
c) $((p \wedge q) \rightarrow (- q \rightarrow - p))$
d) $((p \veebar q) \wedge (- p \wedge - q))$

10) Em cada item abaixo, verifique se ocorre equivalência lógica ou implicação lógica entre as fórmulas dadas:
a) $(p \wedge (p \vee q))$ e p
b) p e $(p \veebar q)$
c) $(p \wedge (p \rightarrow q))$ e q
d) $(p \vee (p \wedge q))$ e p
e) $((p \rightarrow q) \rightarrow q)$ e p
f) $(p \rightarrow q)$ e $(- p \vee q)$
g) $(p \rightarrow q)$ e $((q \rightarrow r) \rightarrow (p \rightarrow r))$
h) $(p \leftrightarrow q)$ e $((p \wedge q) \vee (- p \wedge - q))$
i) $(p \rightarrow q)$ e $((- p \rightarrow q) \rightarrow q)$
j) $(q \rightarrow p)$ e $(- q \vee p)$
k) $(p \vee (q \vee r))$ e $((q \vee (p \vee r)) \vee p)$
l) $(p \rightarrow q)$ e $- (p \wedge - q)$
m) $(p \vee q)$ e $(- p \rightarrow q)$
n) q e $(p \wedge (p \rightarrow q))$
o) $((p \veebar q) \wedge - q)$ e p
p) $(p \leftrightarrow q)$ e $(q \leftrightarrow p)$
q) $(p \leftrightarrow q)$ e $(- p \leftrightarrow - q)$
r) $(p \vee q)$ e $- (- p \wedge - q)$
s) $(p \wedge q)$ e $- (- p \vee - q)$

3

Construção e simplificação de fórmulas e formas normais

As equivalências lógicas entre fórmulas nos mostram que fórmulas que possuem os mesmos valores lógicos, para todas atribuições de valores verdade feitas às suas variáveis proposicionais, podem ser escritas de maneiras diferentes.

Para toda fórmula podemos, mediante transformações que resultam em equivalência lógica, chegar a uma forma normal conjuntiva ou a uma forma normal disjuntiva, as quais apresentam certos padrões muito utilizados em aplicações da Lógica Matemática como construção de algoritmos ou desenvolvimento de circuitos eletroeletrônicos. Porém, antes de estudarmos estas formas, veremos o tópico construção de fórmulas, o qual nos permitirá obter uma fórmula para uma tabela de verdade conhecida.

Cabe ressaltar que tabelas de verdade surgem na modelagem de problemas de diversas áreas. Exemplo: considere o problema de controlar o funcionamento de uma bomba abastecida em três entradas, levando em conta que ela só pode ser acionada se pelo menos duas das três entradas estiverem em funcionamento. Assim, se chamarmos essas entradas de p, q e r e o acionamento da bomba de A, essa situação é representada pela tabela:

p	q	r	A
V	V	V	V
V	V	F	V
V	F	V	V
V	F	F	F
F	F	F	F
F	F	V	F
F	V	F	F
F	V	V	V

e assim necessitamos obter a fórmula A que controlará o acionamento da bomba.

3.1 Construção de fórmulas

Já vimos que dada uma fórmula, podemos construir sua tabela de verdade. Agora inverteremos esse processo, isto é, construiremos uma fórmula cujos valores lógicos sejam os de uma determinada tabela. Citaremos dois processos, extremamente simples.

Primeiro processo: Seja A a fórmula procurada. Para construir a fórmula desejada, escrevemos inicialmente uma fórmula para cada linha da tabela dada que contenha o valor lógico verdadeiro (V) na coluna dos vl(A). Estas fórmulas parciais são formadas pela conjunção das variáveis proposicionais negadas ou não, usando-se a própria variável proposicional quando o seu valor verdade for verdadeiro (V), ou a sua negação quando o seu valor verdade for falso (F). Finalmente, obtém-se a fórmula procurada reunindo-se todas as fórmulas parciais, através da disjunção inclusiva. As fórmulas obtidas por este processo possuem uma forma especial, denominada Forma Normal Disjuntiva Padronizada.

Segundo processo: Seja A a fórmula procurada. Para construir a fórmula desejada, escrevemos inicialmente uma fórmula para cada linha da tabela dada que contenha o valor lógico falso (F) na coluna dos vl(A). Estas fórmulas parciais são formadas pela disjunção inclusiva das variáveis proposicionais negadas ou não, usando-se a própria variável proposicional quando o seu valor verdade for falso (F), ou a sua negação quando o seu valor verdade for verdadeiro (V). Finalmente, obtém-se a fórmula procurada reunindo-se todas as fórmulas parciais, através da conjunção. As fórmulas obtidas por este processo possuem uma forma especial, denominada Forma Normal Conjuntiva Padronizada.

Observações:

1) Quando a tabela de verdade dada representar uma tautologia ou uma contradição, basta lembrarmos que já conhecemos fórmulas deste tipo bastante simples.

2) Se desejarmos utilizar os conectivos não citados no processo acima, isto será possível através das equivalências lógicas.

3) É claro que a fórmula obtida pelo primeiro processo e a fórmula obtida pelo segundo processo são logicamente equivalentes.

Exemplo: Consideremos a seguinte tabela de verdade:

p	q	A
V	V	F
V	F	V
F	V	V
F	F	F

Usando-se a primeira regra proposta, obtemos que as fórmulas parciais são $(p \wedge - q)$ para a segunda linha e $(- p \wedge q)$ para a terceira linha. Finalmente obtemos que a fórmula A procurada é $((p \wedge - q) \vee (- p \wedge q))$.

Usando-se a segunda regra proposta, obtemos que as fórmulas parciais são $(- p \vee - q)$ para a primeira linha e $(p \vee q)$ para a quarta linha. Finalmente obtemos que a fórmula A procurada é $((- p \vee - q) \wedge (p \vee q))$.

Exemplo: Consideremos agora a tabela de verdade:

p	q	r	A
V	V	V	V
V	V	F	V
V	F	V	V
V	F	F	V
F	F	F	F
F	F	V	F
F	V	F	F
F	V	V	F

Usando-se a primeira regra dada acima, obtemos que as fórmulas parciais são $(p \wedge q \wedge r)$, $(p \wedge q \wedge - r)$, $(p \wedge - q \wedge r)$ e $(p \wedge - q \wedge - r)$ para a primeira, segunda, terceira e quarta linhas respectivamente. Finalmente obtemos que a fórmula A procurada é

$$(p \wedge q \wedge r) \vee (p \wedge q \wedge - r) \vee (p \wedge - q \wedge r) \vee (p \wedge - q \wedge - r).$$

Os procedimentos estudados, em geral, nos conduzem a fórmulas bastante longas. Devemos então, sempre que possível, simplificá-las, o que pode ser feito através da aplicação de equivalências lógicas. Para isto, é interessante observar que, sendo A uma fórmula qualquer, C uma contradição e T uma tautologia então $(A \wedge C)$ eq C e $(A \vee T)$ eq T.

Consideremos então a fórmula obtida no último exemplo:

$$(p \wedge q \wedge r) \vee (p \wedge q \wedge - r) \vee (p \wedge - q \wedge r) \vee (p \wedge - q \wedge - r).$$

Utilizando as equivalências notáveis "Leis Distributivas" e "Leis Associativas", obtemos:

$$p \wedge ((q \wedge r) \vee (q \wedge - r) \vee (- q \wedge r) \vee (- q \wedge - r)).$$

Utilizando novamente a equivalência notável "Leis Distributivas" obtemos:

$$p \wedge ((q \wedge (r \vee - r)) \vee (- q \wedge (r \vee - r)).$$

Como $(r \vee - r)$ eq T, em que T é tautologia, temos:

$$p \wedge ((q \wedge T) \vee (- q \wedge T)).$$

Agora $(q \wedge T)$ eq q e $(- q \wedge T)$ eq - q, e assim temos:

$$p \wedge (q \vee - q).$$

Como $(q \vee - q)$ eq T, temos:

$$p \wedge T \text{ eq } p.$$

Assim, demonstramos que a fórmula:

$(p \wedge q \wedge r) \vee (p \wedge q \wedge - r) \vee (p \wedge - q \wedge r) \vee (p \wedge - q \wedge - r).$

é logicamente equivalente à fórmula:

$$p,$$

muito mais simples.

Exemplo: Consideremos a seguinte tabela de verdade:

P	q	A
V	V	V
V	F	F
F	V	F
F	F	V

Usando-se a segunda regra proposta, obtemos que as fórmulas parciais são $(- p \vee q)$ para a segunda linha e $(p \vee - q)$ para a terceira linha. Finalmente obtemos que a fórmula A procurada é $((- p \vee q) \wedge (p \vee - q))$.

Pela equivalência notável, "Leis Distributivas", obtemos:

$$((- p \vee q) \wedge p) \vee ((- p \vee q) \wedge - q)).$$

Pela equivalência notável, "Leis Comutativas", obtemos:

$$(p \wedge (- p \vee q)) \vee (- q \wedge (- p \vee q)).$$

E novamente pela equivalência notável "Leis Distributivas", obtemos:

$$((p \wedge - p) \vee (p \wedge q)) \vee ((- q \wedge - p) \vee (- q \wedge q)).$$

Como $(p \wedge - p)$ eq C e $(- q \wedge q)$ eq C, em que C é contradição, temos:

$$(C \vee (p \wedge q)) \vee ((- q \wedge - p) \vee C).$$

E, finalmente, como $(C \vee (p \wedge q))$ eq $(p \wedge q)$ e $((- q \wedge - p) \vee C)$ eq $(- q \wedge - p)$ temos:

$$(p \wedge q) \vee (- q \wedge - p).$$

Exemplo: Considere a tabela de verdade:

p	q	r	A
V	V	V	V
V	V	F	V
V	F	V	V
V	F	F	F
F	F	F	F
F	F	V	V
F	V	F	V
F	V	V	V

Para esta tabela, o segundo procedimento é mais adequado, pois existem apenas dois valores lógicos F. Utilizando-se então este procedimento, obtemos as seguintes fórmulas parciais para a quarta e para a quinta linha, respectivamente:

$$(- p \vee q \vee r) \text{ e } (p \vee q \vee r).$$

Assim a fórmula final é:

$$(- p \vee q \vee r) \wedge (p \vee q \vee r).$$

Utilizando a equivalência notável "Leis Comutativas", obtemos:

$$(q \vee r \vee - p) \wedge (q \vee r \vee p).$$

Pela equivalência notável "Leis Distributivas", obtemos:

$$(q \vee r) \vee (- p \wedge p).$$

Como $(- p \wedge p)$ eq C, em que C é contradição, obtemos:

$$(q \vee r) \vee C \text{ eq } (q \vee r).$$

Assim obtemos a fórmula:

$$(q \vee r),$$

que é muito mais simples que a fórmula:

$$(- p \vee q \vee r) \text{ e } (p \vee q \vee r).$$

3.2 Um exemplo real: Projetando circuitos lógicos combinacionais

Quando o nível lógico de saída de um circuito lógico é dado para todas as combinações possíveis das entradas, então o resultado pode ser colocado em uma tabela verdade.

Considere então o problema de projetar um circuito lógico que tem três entradas A, B e C e uma saída X que será ALTA somente quando a maioria das entradas é ALTA.

O problema estabelece que a saída X será 1 (que é o mesmo que V no Cálculo Proposicional) quando duas ou mais entradas forem iguais a 1 e para todos os outros casos a saída X será igual a 0 (que é o mesmo que F no Cálculo Proposicional):

A	B	C	X
1	1	1	1
1	1	0	1
1	0	1	1
1	0	0	0
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1

Usando-se a primeira regra para a construção de fórmulas, obtemos que as fórmulas parciais são $(A \wedge B \wedge C)$, $(A \wedge B \wedge - C)$, $(A \wedge - B \wedge C)$ e $(- A \wedge B \wedge C)$ para a primeira, segunda, terceira e oitava linhas, respectivamente. Finalmente obtemos que a fórmula X procurada é:

$$(A \wedge B \wedge C) \vee (A \wedge B \wedge - C) \vee (A \wedge - B \wedge C) \vee (- A \wedge B \wedge C).$$

Que pela equivalência notável “Leis Associativas” é o mesmo que:

$$(A \wedge B \wedge C) \vee (((A \wedge B \wedge - C) \vee (A \wedge - B \wedge C)) \vee (- A \wedge B \wedge C)).$$

Daí, pelas equivalências notáveis “Leis idempotentes” e “Leis Distributivas” obtemos:

$$(((A \wedge B \wedge C) \vee (A \wedge B \wedge - C)) \vee ((A \wedge B \wedge C) \vee (A \wedge - B \wedge C))) \vee ((A \wedge B \wedge C) \vee (- A \wedge B \wedge C))).$$

Pelas equivalências notáveis “Leis Distributivas” e “Leis Comutativas” obtemos:

$$(((A \wedge B) \wedge (C \vee - C)) \vee ((A \wedge C) \wedge (B \vee - B)) \vee ((B \wedge C) \wedge (A \vee - A))).$$

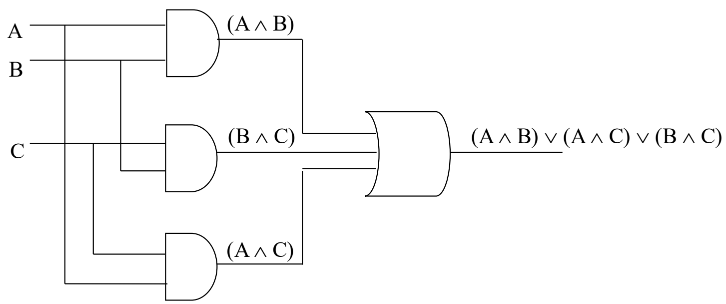
Agora: $(C \vee - C)$ eq $(B \vee - B)$ eq $(A \vee - A)$ eq 1. Logo temos:

$$(((A \wedge B) \wedge 1) \vee ((A \wedge C) \wedge 1) \vee ((B \wedge C) \wedge 1)).$$

Também $(((A \wedge B) \wedge 1)$ eq $(A \wedge B)$, $((A \wedge C) \wedge 1)$ eq $(A \wedge C)$ e $((B \wedge C) \wedge 1))$ eq $(B \wedge C)$. Logo obtemos:

$$(A \wedge B) \vee (A \wedge C) \vee (B \wedge C) .$$

Assim, o circuito terá três portas AND (conjunção, no Cálculo Proposicional) e duas portas OR (disjunção inclusiva, no Cálculo Proposicional). Usualmente, no estudo de circuitos a conjunção é representada pelo ponto, símbolo da multiplicação e a disjunção inclusiva é representada pelo símbolo da adição. Graficamente, temos a seguinte representação:



Observe que este exemplo possui a mesma tabela que o nosso exemplo da bomba do início deste capítulo. Assim, naquele, o tratamento seria idêntico ao neste realizado.

3.3 Formas normais

As fórmulas obtidas pelos dois processos estudados possuem formas especiais, as quais recebem o nome de Formas Normais, que por nós serão estudadas a seguir. Antes, lembramos que essas formas, como já dissemos, em geral necessitam de simplificação, para o que já os conhecemos a forma algébrica. Isto se dá através das equivalências lógicas, às vezes não muito agradáveis, e por isso estudaremos também um processo gráfico para a simplificação de fórmulas, denominado diagramas de Karnaugh.

3.3.1 Forma normal conjuntiva

Definição: Uma fórmula se encontra na *forma normal conjuntiva* (FNC) quando contém somente os conectivos disjunção inclusiva ($\vee$), conjunção ($\wedge$), e negação (-); quando nenhum conectivo - afeta nenhum conectivo $\vee$, $\wedge$, ou -; e quando finalmente nenhum conectivo $\vee$ afeta a nenhum conectivo $\wedge$. Isto é, uma fórmula na forma normal conjuntiva é uma conjunção:

$$C_1 \wedge C_2 \wedge \cdots \wedge C_n$$

em que cada C_i, para $i = 1, \cdots, n$ é, usualmente, uma disjunção inclusiva de variáveis proposicionais ou de negações destas. Em certos casos algum C_i pode ser formado apenas por uma variável proposicional ou negação de variável proposicional.

Além disso, se cada C_i, para $i = 1, \cdots, n$ possuir todas as variáveis proposicionais envolvidas na fórmula, ou suas negações, então estes recebem o nome maxtermo (M) e dizemos que a fórmula está na *forma normal conjuntiva padronizada.*

3.3.1.1 Transformação de uma fórmula para a forma normal conjuntiva

Quando estudamos a construção de fórmulas, vimos que dada uma tabela de verdade, o segundo processo para a construção de uma fórmula que represente esta tabela nos conduz a uma fórmula na forma normal conjuntiva padronizada. Sendo assim, dada uma fórmula, um procedimento para obter sua forma normal conjuntiva é construir a sua tabela de verdade e aplicar este processo. Este procedimento, no entanto, torna-se exaustivo ou mesmo impraticável quando o número de variáveis proposicionais é grande. Vamos então introduzir um procedimento que é baseado nas equivalências lógicas.

Seja A uma fórmula, os itens seguintes transformam a fórmula A para uma fórmula logicamente equivalente na forma normal conjuntiva:

1) Os conectivos, disjunção exclusiva ($x\vee$), condicional ($\rightarrow$) e bicondicional ($\leftrightarrow$), que porventura existam na fórmula A, devem ser eliminados, utilizando-se equivalências lógicas. Para qualquer fórmula parcial de A do tipo $B \; x\vee \; C$ deve-se fazer a substituição pela fórmula logicamente equivalente - $(B \leftrightarrow C)$; para qualquer fórmula parcial de A do tipo $B \rightarrow C$ deve-se fazer a substituição pela fórmula logicamente equivalente - $B \vee C$ e qualquer fórmula parcial de A do tipo $B \leftrightarrow C$ deve-se fazer a

substituição pela fórmula logicamente equivalente $(- B \vee C) \wedge (- C \vee B)$;

2) O conectivo negação (-) deve ocupar uma posição especial, isto é, o mais interno possível na fórmula. Deste modo, as fórmulas parciais de A do tipo $- (B \wedge C)$ e $- (B \vee C)$ devem ser substituídas pelas fórmulas logicamente equivalentes $- B \vee - C$ e $- B \wedge - C$, respectivamente;

3) Em consequência do item 2, o conectivo negação (-) se encontrará, às vezes, de maneira múltipla ante às variáveis proposicionais, e isto deve ser evitado. Substituiremos toda variável proposicional com um número par de sinais de negação, antepostos a ela, pela variável proposicional sozinha, isto é, sem sinal de negação anteposto a ela, e substituiremos toda variável proposicional com um número ímpar de sinais de negação, antepostos a ela, pela variável proposicional negada, isto é, com um único sinal de negação anteposto a ela;

4) Depois dos três passos anteriores, nos encontramos com uma fórmula formada por variáveis proposicionais negadas ou não negadas acompanhadas de $\vee$ e $\wedge$. Devemos evitar que o conectivo disjunção inclusiva ($\vee$) afete algum conectivo conjunção ($\wedge$). Para isto, toda fórmula parcial de do tipo $B \vee (C \wedge D)$ será substituída pela fórmula logicamente equivalente $(B \vee C) \wedge (B \vee D)$, e toda fórmula parcial do tipo $(C \wedge D) \vee B$ será substituída pela fórmula logicamente equivalente $(C \vee B) \wedge (D \vee B)$.

Exemplo: Passe a fórmula $- (((p \vee q) \wedge - q) \vee (r \wedge q))$ para a FNC.

1) Não temos os conectivos condicional ($\rightarrow$) e bicondicional ($\leftrightarrow$)

2) $- ((p \vee q) \wedge - q) \wedge - (r \wedge q)$

$(- (p \vee q) \vee - - q) \wedge (- r \vee - q)$

$((- p \wedge - q) \vee - - q) \wedge (- r \vee - q)$

3) $((- p \wedge - q) \vee q) \wedge (- r \vee - q)$

4) $(- p \vee q) \wedge (- q \vee q) \wedge (- r \vee - q)$, que está na FNC.

3.3.2 Forma normal disjuntiva

Definição: Uma fórmula se encontra na *forma normal disjuntiva* (FND) quando contém somente os conectivos disjunção inclusiva ($\vee$), conjunção ($\wedge$), e negação (-), quando nenhum conectivo - afeta nenhum conectivo $\vee$, $\wedge$, ou -, e quando finalmente, nenhum conectivo $\wedge$, afeta a nenhum conectivo $\vee$. Isto é, uma fórmula na forma normal disjuntiva é uma disjunção:

$$C_1 \wedge C_2 \wedge \cdots \wedge C_n$$

em que cada C_i, para $i = 1,\cdots,n$, é, usualmente, uma conjunção de variáveis proposicionais ou de negações destas. Em certos casos algum C_i pode ser formado apenas por uma variável proposicional ou negação de variável proposicional.

Além disso, se cada C_i para $i = 1,\cdots,n$ possuir todas as variáveis proposicionais envolvidas na fórmula (ou suas negações), então estes recebem o nome mintermo (m) e dizemos que a fórmula está na *forma normal disjuntiva padronizada.*

3.3.2.1 Transformação de uma fórmula para a forma normal disjuntiva

Quando estudamos a construção de fórmulas, vimos que dada uma tabela de verdade, o primeiro processo para a construção de uma fórmula que represente esta tabela nos conduz a uma fórmula na forma normal disjuntiva padronizada. Sendo assim, dada uma fórmula, um procedimento para obter sua forma normal disjuntiva é construir a sua tabela de verdade e aplicar este processo. Este procedimento, no entanto, torna-se exaustivo ou mesmo impraticável quando o número de variáveis proposicionais é grande. Vamos então introduzir um procedimento que é baseado nas equivalências lógicas.

Seja A uma fórmula, para transformá-la em uma fórmula logicamente equivalente na forma normal disjuntiva os passos 1, 2 e 3 a serem executados são os mesmos da transformação para a forma normal conjuntiva, e por isso não serão novamente apresentados, mas devem ser executados, nessa ordem, antecedendo o quarto passo abaixo apresentado.

4) Depois dos três passos anteriores, nos encontramos com uma fórmula formada por variáveis proposicionais negadas ou não negadas acompanhadas de $\vee$ e $\wedge$. Devemos evitar que o conectivo conjunção ($\wedge$) afete algum conectivo disjunção inclusiva ($\vee$). Para isto, toda fórmula parcial de do tipo $B \wedge (C \vee D)$ será substituída pela fórmula logicamente equivalente

$(B \wedge C) \vee (B \wedge D)$, e toda fórmula parcial do tipo $(C \vee D) \wedge B$ será substituída pela fórmula logicamente equivalente $(C \wedge B) \vee (D \wedge B)$.

Exemplo: Passe a fórmula $- (((p \vee q) \wedge - q) \vee (r \wedge q))$ para a FND.

1) Não temos os conectivos condicional ($\rightarrow$) e bicondicional ($\leftrightarrow$)

2) $- ((p \vee q) \wedge - q) \wedge - (r \wedge q)$

$(- (p \vee q) \vee - - q) \wedge (- r \vee - q)$

$((- p \wedge - q) \vee - - q) \wedge (- r \vee - q)$

3) $((- p \wedge - q) \vee q) \wedge (- r \vee - q)$

4) $(((- p \wedge - q) \vee q) \wedge - r) \vee (((- p \wedge - q) \vee q) \wedge - q)$

$((- p \wedge - q) \wedge - r) \vee (q \wedge - r) \vee ((- p \wedge - q) \wedge - q) \vee (q \wedge - q)$

$- p \wedge - q \wedge - r) \vee (q \wedge - r) \vee (- p \wedge - q \wedge - q) \vee (q \wedge - q)$, que está na FND.

Observações:

1) As transformações usadas resultam em equivalência lógica, e isto pode ser comprovado por meio de tabelas de verdade.

2) Toda fórmula pode ser transformada para a FNC e para a FND.

3) Os itens 1, 2 e 3 são os mesmos para ambas as transformações, para a FNC e para a FND.

4) Uma fórmula na FNC será uma tautologia sempre que em cada membro da conjunção (conjuntivo) existir uma variável proposicional e sua negação como membros da disjunção inclusiva (disjuntivo).

5) Uma fórmula na FND será uma contradição sempre que, em cada membro da disjunção inclusiva (disjuntivo), existir uma variável proposicional e sua negação como membros da conjunção (conjuntivo).

6) Quando necessário, em ambas as transformações, o que estudamos sobre parênteses deverá ser considerado.

7) A utilização das “Leis Comutativas” e “Leis Distributivas” convenientemente transformam uma fórmula da FNC para a FND e vice-versa.

3.3.3 Simplificação de fórmulas através dos diagramas de Karnaugh

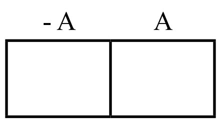
Como o leitor observou, os procedimentos para a construção de fórmulas ou de transformação de fórmulas para as formas normais conjuntiva ou disjuntiva geralmente nos conduzem a fórmulas que devem ser simplificadas. Até aqui a simplificação de fórmulas foi realizada mediante a utilização de equivalências lógicas. Agora apresentaremos, de maneira breve, uma opção para a simplificação de fórmulas: os diagramas de Karnaugh.

Os diagramas de Karnaugh[2] são bastante utilizados para a simplificação de fórmulas nas formas normais padronizadas, com duas, três, quatro, cinco ou mais variáveis, sendo que para cada caso existe um tipo de diagrama mais apropriado.

Para o restante deste capítulo o termo *variável* representará uma fórmula qualquer, e será denotada por letras maiúsculas do alfabeto, podendo assim ser simplesmente uma variável proposicional do Cálculo Proposicional, e deixamos por conta do leitor refletir se os diagramas de Karnaugh são aplicáveis quando estas variáveis não são simplesmente variáveis proposicionais.

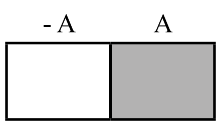
3.3.3.1 Diagrama de Karnaugh para 1 variável

Para uma variável, temos o seguinte diagrama:



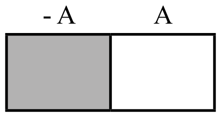
No quadro, temos as regiões da variável A:

A região onde vl(A) = V é:



2 Mais sobre diagramas de Karnaugh pode ser encontrado no livro *Lógica e álgebra de Boole*, de Jacob Daghlian.

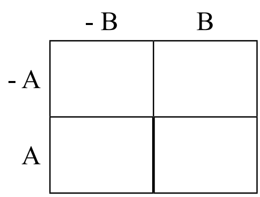
A região onde vl(A) = F (ou vl(- A) = V) é:



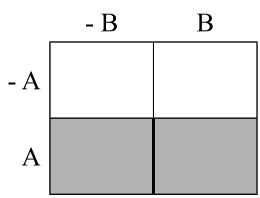
Observe que toda fórmula que contém uma única variável proposicional, digamos p, é logicamente equivalente à p, ou à - p, ou à p $\vee$ - p (aquelas que são tautologias), ou à p $\wedge$ - p (aquelas que são contradições). Portanto, os diagramas de Karnaugh para uma variável proposicional são dispensáveis.

3.3.3.2 Diagrama de Karnaugh para 2 variáveis

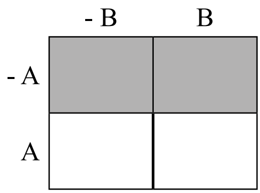
Para duas variáveis, temos o seguinte diagrama:



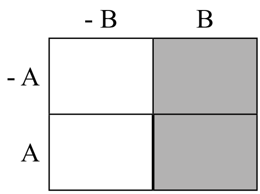
No quadro, temos as regiões das variáveis A e B:
A região onde vl(A) = V é:



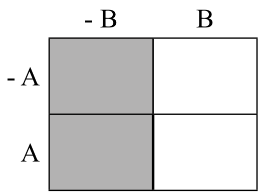
A região onde vl(A) = F (ou vl(- A) = V) é:



A região onde vl(B) = V é:



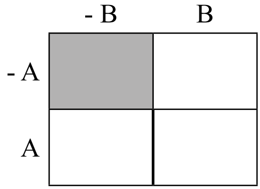
A região onde vl(B) = F (ou vl(- B) = V)



Com duas variáveis, podemos obter 4 possibilidades:

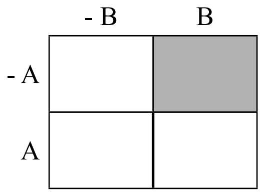
A	B	
V	V	Caso 0
V	F	Caso 1
F	V	Caso 2
F	F	Caso 3

No caso 3, temos vl(A) = F e vl(B) = F. A região do diagrama que mostra esta condição é a obtida da intersecção das regiões onde vl(A) = F e vl(B) = F. A intercessão destas regiões é:



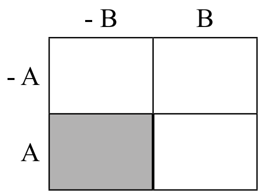
Esta região é chamada de região (- A $\wedge$ - B).

No caso 2, temos vl(A) = F e vl(B) = V. A região do diagrama que mostra esta condição é a da intersecção das regiões onde vl(A) = F (ou vl(- A) = V) e vl(B) = V. Fazendo esta intersecção, temos:



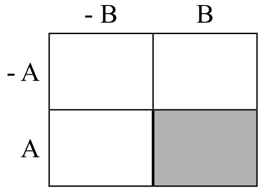
Esta região é chamada de região (- A $\wedge$ B).

No caso 1, temos a intersecção das regiões onde vl(A) = V e vl(B) = F (ou vl(- B) = V). Fazendo esta intersecção, temos:



Esta região é chamada de região (A $\wedge$ - B).

No caso 0, temos a intersecção das regiões onde vl(A) = V e vl(B) = V. Fazendo esta intersecção, temos:



Esta região é chamada de região (A $\wedge$ B).

Podemos distribuir, então, as 4 possibilidades neste diagrama, da seguinte forma:

	- B	B
- A	Caso 3	Caso 2
A	Caso 1	Caso 0

Logo, notamos que cada linha da tabela da verdade possui sua região própria no diagrama de Karnaugh. Essas regiões são, portanto, os locais onde devem ser colocados os valores que a fórmula assume nas diferentes possibilidades.

Para entendermos melhor o significado deste conceito, vamos utilizar um exemplo:

A tabela de verdade abaixo mostra o estudo de uma fórmula S de duas variáveis. Vamos colocar seus resultados no diagrama de Karnaugh.

A	B	S	
V	V	V	Caso 0
V	F	V	Caso 1
F	V	V	Caso 2
F	F	F	Caso 3

Utilizando o primeiro processo de construção de fórmulas, obtemos a seguinte fórmula:

$$(A \wedge B) \vee (A \wedge - B) \vee (- A \wedge B),$$

que está na forma normal disjuntiva padronizada.

Primeiramente, vamos colocar no diagrama o que a fórmula S assume no caso 3, ou seja, vamos colocar o valor que a fórmula S assume para este caso na região (- A ∧ - B):

	- B	B
- A	F	
A		

Agora, vamos colocar no diagrama o valor que a fórmula S assume no caso 2 na região (- A ∧ B):

	- B	B
- A		V
A		

Em seguida vamos colocar no diagrama o valor que a fórmula S assume no caso 1 na região (A ∧ - B):

	- B	B
- A		
A	V	

E, finalmente, colocamos no diagrama o valor que a fórmula S assume no caso 0 na região (A ∧ B):

	- B	B
- A		
A		V

Temos, agora, a tabela de verdade a fórmula $(A \wedge B) \vee (A \wedge - B) \vee (- A \wedge B)$, descrita no diagrama de Karnaugh:

	- B	B
- A	F	V
A	V	V

Uma vez entendida a colocação dos valores assumidos pela fórmula em cada caso no diagrama de Karnaugh, para efetuar a simplificação de uma fórmula S na forma normal disjuntiva padronizada utilizamos o seguinte método:

- Tentamos agrupar as regiões onde vl(S) = V, no menor número possível de grupos, onde um *grupo* é o conjunto de, no máximo, duas regiões onde vl(S) = V, e no caso de duas regiões, estas tem um lado em comum, ou seja, são *adjacentes*.
- As regiões onde vl(S) = V que não puderem ser agrupadas, serão consideradas isoladamente.
- Se necessário, um mesmo valor lógico V pode ser agrupado mais de uma vez.

No exemplo anterior, temos:

	- B	B	
- A	F	V	
A	V	V	grupo 1

grupo 2

A variável (ou negação de variável) que se repetir em cada grupo permanece na fórmula. A variável que não se repete é eliminada.

A fórmula simplificada será a disjunção inclusiva da conjunção (pois estamos trabalhando com uma fórmula na forma normal disjuntiva padronizada) das variáveis (ou negação de variáveis) que permanecerem na fórmula.

No exemplo, nenhum valor lógico V ficou fora dos grupos. No grupo 1 a variável que se repete é a variável A, e no grupo 2 a variável que se repete é a variável B.

Assim, a fórmula S simplificada que desejamos é:

$$A \vee B.$$

Como permaneceu apenas uma variável em cada grupo, a conjunção não foi utilizada.

Como podemos notar, esta é a disjunção inclusiva entre A e B, concordando com a tabela de verdade deste exemplo. Outro fato a ser notado é que a fórmula obtida, diretamente da tabela da verdade, é visivelmente maior que a fórmula minimizada.

Para uma fórmula S na forma normal conjuntiva padronizada, os passos para a sua simplificação são os seguintes:

- Tentamos agrupar as regiões onde vl(S) = F, no menor número possível de grupos, onde um *grupo* é o conjunto de, no máximo, duas regiões onde vl(S) = F, e no caso de duas regiões, estas tem um lado em comum, ou seja, são *adjacentes*.
- As regiões onde vl(S) = F que não puderem ser agrupadas, serão consideradas isoladamente.
- Se necessário, um mesmo valor lógico F pode ser agrupado mais de uma vez.

Para cada variável (ou negação de variável) que se repetir em cada grupo permanecerá na fórmula a sua negação. A variável que não se repete é eliminada.

A fórmula simplificada será a conjunção da disjunção inclusiva da negação (pois estamos trabalhando com uma fórmula na forma normal conjuntiva padronizada) das variáveis (ou negação de variáveis) que permanecerem na fórmula.

Exemplo: Vamos simplificar a fórmula da tabela de verdade abaixo:

A	B	S
V	V	V
V	F	F
F	V	F
F	F	F

Obtendo a fórmula S diretamente da tabela, pelo segundo processo de construção de fórmulas, obtemos:

$$(- A \vee B) \wedge (A \vee - B) \wedge (A \vee B),$$

que está na forma normal conjuntiva padronizada.

Transportando a tabela para o diagrama, mediante processo já visto, obtemos:

	- B	B
- A	F	F
A	V	V

Agora, vamos agrupar os valores lógicos F:

	- B	B
- A	F	F
A	F	V

grupo 1

grupo 2

No grupo 1, a variável que se repete é a variável - A. E no grupo 2, a variável que se repete é a variável - B, assim permanecerão na fórmula - - A e - - B, ou seja A e B.

Logo, a fórmula simplificada é:

$$A \wedge B.$$

Como permaneceu apenas uma variável em cada grupo, a disjunção inclusiva não foi utilizada.

3.3.3.3 Diagrama alternativo de Karnaugh para 2 variáveis

Para duas variáveis, temos também o seguinte diagrama alternativo:

A e B

A e B	A e - B	- A e - B	- A e B
Caso 0	Caso 1	Caso 2	Caso 3

concordando com a tabela:

A	B	
V	V	Caso 0
V	F	Caso 1
F	V	Caso 2
F	F	Caso 3

Os quadrados que possuem um lado em comum são adjacentes, e neste diagrama consideramos também o primeiro (Caso 0) e o último (Caso 2) como adjacentes.

Os quadrados adjacentes diferem apenas por uma variável ou pela negação de uma variável.

Observe a sequência dos casos neste diagrama: Caso 0, Caso 1, Caso 3 e Caso 2 e que, ao passarmos de um quadrado para outro adjacente, somente uma variável muda de valor lógico.

3.3.3.4 Diagrama de Karnaugh para 3 variáveis

Para três variáveis, temos o seguinte diagrama:

C \ A e B	A e B	A e - B	- A e - B	- A e B
	Caso 0	Caso 2	Caso 5	Caso 7
C	Caso 1	Caso 3	Caso 4	Caso 6

concordando com a tabela:

A	B	C	
V	V	V	Caso 0
V	V	F	Caso 1
V	F	V	Caso 2
V	F	F	Caso 3
F	F	F	Caso 4
F	F	V	Caso 5
F	V	F	Caso 6
F	V	V	Caso 7

Um quadrado de cima e o logo abaixo dele são adjacentes (os casos 2 e 3 por exemplo) e um quadrado e o logo a sua direita também são adjacentes (os casos 2 e 5 por exemplo). Neste diagrama consideramos também o primeiro (Caso 0) e o último (Caso 7) superiores e o primeiro (Caso 1) e o último (Caso 6) inferiores como adjacentes.

Os quadrados adjacentes diferem apenas por uma variável ou pela negação de uma variável.

Observe a sequência dos casos neste diagrama.

Portanto, ao passarmos de um quadrado para outro adjacente, somente uma variável muda de valor lógico.

Para efetuar a simplificação de fórmulas na forma normal disjuntiva padronizada, utilizamos o seguinte método:

- Agrupamos as regiões onde o valor lógico é V, para formar grupos de 2^n (1, 2 ou 4, pois para 8 valores lógicos V temos uma tautologia) valores lógicos V, no menor número possível de grupos.

- As regiões onde os valores lógicos V não puderem ser agrupadas, serão consideradas isoladamente.
- Se necessário, um mesmo valor lógico V pode ser agrupado mais de uma vez.

As variáveis (ou negação de variáveis) que se repetirem em cada grupo permanecem na fórmula. As variáveis que não se repetem são eliminadas.

A fórmula simplificada será a disjunção inclusiva da conjunção (pois estamos trabalhando com uma fórmula na forma normal disjuntiva padronizada) das variáveis (ou negação de variáveis) que permanecerem na fórmula.

Exemplo: Construindo o diagrama de Karnaugh para a fórmula

$$(A \wedge B \wedge C) \vee (A \wedge - B \wedge - C) \vee (- A \wedge B \wedge C),$$

que está na forma normal disjuntiva padronizada obtemos:

A e B / C	A e B	A e - B	- A e B	- A e - B
C	V	F	F	V
	F	V	F	F

Assim, a fórmula simplificada é:

$$(B \wedge C) \vee (A \wedge - B \wedge - C).$$

Para simplificar uma fórmula S na forma normal conjuntiva padronizada, utilizamos o seguinte método:

- Agrupamos as regiões onde o valor lógico é F, para formar grupos de 2^n (1, 2 ou 4, pois para 8 valores lógicos F temos uma contradição) valores lógicos F, no menor número possível de grupos.
- As regiões onde os valores lógicos F não puderem ser agrupadas, serão consideradas isoladamente.
- Se necessário, um mesmo valor lógico F pode ser agrupado mais de uma vez.

Para cada variável (ou negação de variável) que se repetir em cada grupo permanecerá na fórmula a sua negação. As variáveis que não se repetem são eliminadas.

A fórmula simplificada será a conjunção da disjunção inclusiva (pois estamos trabalhando com uma fórmula na forma normal conjuntiva padronizada) das variáveis (ou negação de variáveis) que permanecerem na fórmula.

Exemplo: Construindo o diagrama de Karnaugh para a fórmula:

$$(A \vee B \vee C) \wedge (A \vee - B \vee - C) \wedge (- A \vee B \vee C),$$

que está na forma normal conjuntiva padronizada obtemos:

C \ A e B				
C	V	V	V	F
	V	F	F	V

e assim a fórmula simplificada é:

$$(B \vee C) \wedge (A \vee - B \vee - C).$$

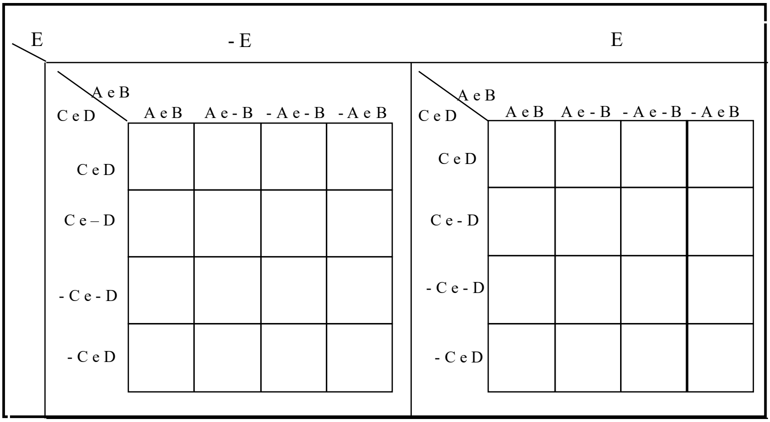
2.3.3.5 Diagrama de Karnaugh para 4 ou mais variáveis

Para quatro variáveis, temos o seguinte diagrama:

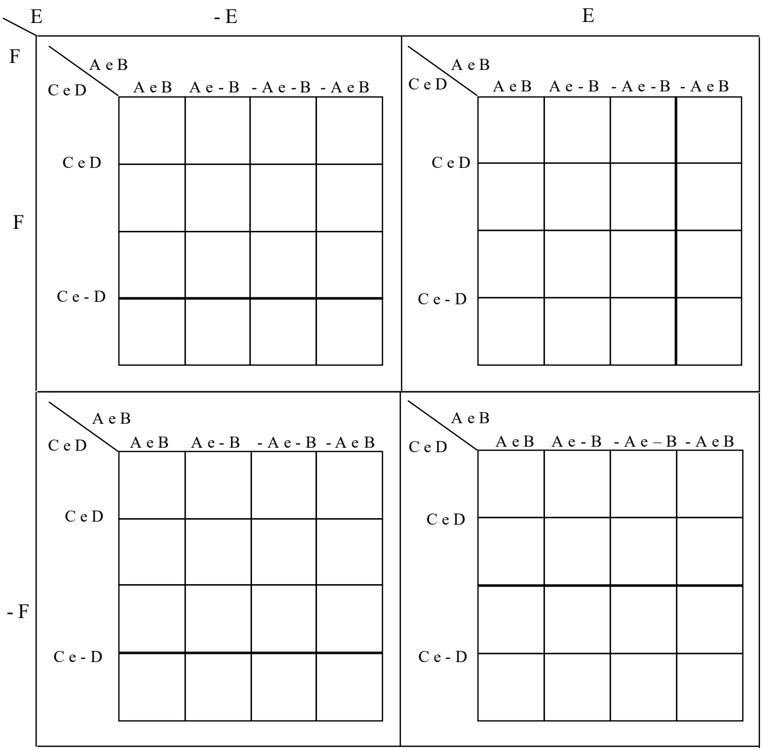
C e D \ A e B	A e B	A e - B	- A e - B	- A e B
C e D				
C e -D				
-C e -D				
-C e D				

O algoritmo para se utilizar este diagrama é o mesmo do diagrama para três variáveis, lembrando que um quadrado de cima e logo abaixo são adjacentes. Um quadrado e o logo à sua direita também são adjacentes, e neste diagrama consideramos também que em cada linha o primeiro e o último quadrado são adjacentes, e também em cada coluna do diagrama o primeiro quadrado e o último quadrado são adjacentes.

Podemos construir diagramas de Karnaugh para cinco variáveis:



ou para seis variáveis:



Como o leitor já deve ter notado, a partir de sete variáveis o processo de representação torna-se bastante complicado, tornando-se impraticável.

3.4 Exercícios propostos

1) Considere a tabela de verdade:

p	q	A
V	V	V
V	F	V
F	V	F
F	F	F

Obtenha uma fórmula A e simplifique-a, se possível.

2) Considere a tabela de verdade:

p	q	r	A
V	V	V	V
V	V	F	V
V	F	V	F
V	F	F	F
F	F	F	F
F	F	V	F
F	V	F	V
F	V	V	V

Obtenha uma fórmula A e simplifique-a, se possível.

3) Verifique sem o uso de tabelas de verdade (ou seja, construindo a FNC ou a FND) se a fórmula dada, em cada item, é uma tautologia, contradição ou contingência:

a) $(p \to q) \vee (q \to p)$

b) $((p \to q) \to p) \to p$
c) $- (p \wedge - q) \to (q \to p)$
d) $(p \to q) \vee p$
e) $((p \to r) \wedge (q \to r) \wedge - r) \to (- p \vee - q)$
f) $p \wedge (p \to q) \wedge - q$
g) $- (p \wedge q) \wedge (r \to - p)$
h) $(p \to (q \to r)) \wedge p \wedge q \wedge - r$
i) $p \wedge - q \wedge - r \wedge - (q \to r)$

4

Regras de inferência ou Regras de dedução

Às vezes, mostrar que uma certa fórmula é uma tautologia, contradição ou contingência, através de tabela de verdade, se torna um procedimento exaustivo. Por exemplo, para uma fórmula com 10 variáveis proposicionais distintas, teremos uma tabela de verdade com 1024 linhas. Por isso, torna-se necessário encontrar um método para podermos decidir o *caráter* de uma certa fórmula dada, isto é, demonstrar que dada fórmula é consequência lógica de um certo conjunto de fórmula(s), e para tanto sabemos que se o valor(es)-lógico(s) da(s) fórmula(s) deste conjunto for(em) verdadeiro(s) (V), então o valor lógico da fórmula dada também deve ser verdadeiro (V).

Por exemplo, vamos supor que estamos interessados em descobrir se a fórmula - p é consequência lógica das seguintes fórmulas $(p_1 \rightarrow q)$, $(r \rightarrow - q)$, r e $(- p_1 \rightarrow - p)$.

Vimos que, sendo $A_1, A_2, \cdots, A_n$ e B fórmulas, dizer que $A_1, A_2, \cdots, A_n \vdash B$ é o mesmo que dizer que $(A_1 \wedge A_2 \wedge \cdots \wedge A_n) \vdash B$, ou que $\vdash ((A_1 \wedge A_2 \wedge \cdots \wedge A_n) \rightarrow B)$. Assim, voltando ao exemplo anterior, para mostrar que a fórmula - p é consequência lógica das fórmulas $(p_1 \rightarrow q)$, $(r \rightarrow - q)$, r e $(- p_1 \rightarrow - p)$, o que de fato ocorre, necessitamos mostrar que:

$$((p_1 \rightarrow q) \wedge (r \rightarrow - q) \wedge r \wedge (- p_1 \rightarrow - p)) \vdash - p$$

que é o mesmo que mostrar que:

$$\vdash (((p_1 \rightarrow q) \wedge (r \rightarrow - q) \wedge r \wedge (- p_1 \rightarrow - p)) \rightarrow - p).$$

Para qualquer uma das opções que escolhamos, teremos que enfrentar um procedimento no mínimo trabalhoso, uma vez que temos nesse simples exemplo quatro variáveis proposicionais envolvidas.

Precisamos então desenvolver uma procedimento mais eficaz para este tipo de verificação.

De agora em diante, neste capítulo, para facilitar a linguagem e a compreensão, quando necessitarmos representar uma fórmula qualquer por uma letra maiúscula do alfabeto acompanhada ou não por índices inferiores que pertençam ao conjunto dos números inteiros não negativos (Z_+) o faremos sem necessariamente definirmos previamente. Isto é, até o momento definíamos, seja A, ou B, $\cdots$, ou Z, acompanhadas ou não por índices inferiores que pertençam ao conjunto dos números inteiros não negativos (Z_+) uma fórmula e de agora em diante, não mais faremos obrigatoriamente esta citação.

Na notação $A_1, A_2, \cdots, A_n \vdash B$, utilizada para indicar que a fórmula B é consequência lógica das fórmulas $A_1, A_2, \cdots, A_n$, as fórmulas $A_1, A_2, \cdots, A_n$ recebem, a partir de agora, o nome de *premissas* ou *hipóteses* e a fórmula B de *conclusão* ou *tese*.

Definição: Um *argumento* é qualquer conjunto de fórmulas do qual se afirme que uma delas é a conclusão e a(s) outra(s) é(são) a(s) premissa(s). Um argumento é *legítimo* ou *válido* se e somente se a conclusão é consequência lógica da(s) premissa(s).

Concordando com a definição e com a nomenclatura logo acima apresentadas, se as fórmulas $A_1, A_2, \cdots, A_n$, B compõem um argumento válido, no qual $A_1, A_2, \cdots, A_n$ são as premissas e B é a conclusão, este argumento será denotado por $A_1, A_2, \cdots, A_n \vdash B$.

Assim, precisamos de um procedimento para tentar mostrar que a(s) premissa(s) ou hipótese(s) implica(m) logicamente a conclusão, ou seja, para verificarmos a validade de um argumento sem construirmos tabelas de verdade. Vamos então, introduzir uma série de regras de inferência ou regras de dedução para tal objetivo.

Definição: Uma *regra de inferência* ou *regra de dedução* é um procedimento capaz de obter uma conclusão a partir de um conjunto de premissa(s) ou hipótese(s) (no mínimo uma) de modo que a seguinte condição seja satisfeita:

- Se o(s) valor(es)-lógico(s) da(s) premissa(s) ou hipótese(s) é(são) verdadeiro(s) (V), então o valor lógico da conclusão que dela(s) se deduz será verdadeiro (V). Em outras palavras, nunca se dá o caso em que o(s) valor(es)-lógico(s) da(s) premissa(s) ou hipótese(s) é(são) verdadeiro(s) (V), e o valor lógico da conclusão é falso (F).

A definição acima nos diz que se obtivermos uma conclusão, a partir de um conjunto de premissa(s), utilizando apenas regras de inferência, a conclusão será consequência lógica da(s) premissa(s).

Enunciaremos agora as *regras de inferência* ou *regras de dedução*, observando que ao invés de usarmos a notação $A_1, A_2, \cdots, A_n \vdash B$, como de costume, usaremos a notação:

$$\begin{array}{c} A_1 \\ A_2 \\ \vdots \\ \underline{A_n} \\ B \end{array}$$

em que a(s) fórmula(s) que está(ão) acima do traço é(são) a(s) premissa(s), e a fórmula abaixo do traço é a conclusão.

Para tanto, sejam então A, B, C, e D fórmulas quaisquer. Valem as seguintes regras:

***Modus Ponens* (MP):**

$$\begin{array}{c} A \\ \underline{A \to B} \\ B \end{array}$$

Modus Tollens (MT):

$$\frac{\begin{array}{c}-B\\ A \to B\end{array}}{-A}$$

Adjunção (A):

$$\frac{\begin{array}{c}A\\ B\end{array}}{A \wedge B}$$

Simplificação (S):

$$\frac{A \wedge B}{A} \qquad \frac{A \wedge B}{B}$$

Modus Tollendo Ponens (TP):

$$\frac{\begin{array}{c}A \vee B\\ -A\end{array}}{B}$$

Lei da Adição (LA):

$$\frac{A}{A \vee B}$$

Silogismo Hipotético (HS):

$$\frac{\begin{array}{c}A \to B\\ B \to C\end{array}}{A \to C}$$

Silogismo Disjuntivo (DS):

$$\frac{\begin{array}{c}A \vee B\\ A \to C\\ B \to D\end{array}}{C \vee D}$$

Observação: Por meio de tabelas de verdade, podemos verificar em todas as regras de inferência que a conclusão é consequência lógica da(s) premissa(s), ou seja, todas as regras de inferência são argumentos legítimos.

Apresentaremos a seguir um esquema de demonstração, isto é, uma sequência de passos lógicos que permitem a partir de premissa(s) obter uma conclusão que se deseja, em que cada passo lógico é permitido por uma regra de inferência ou por uma equivalência lógica.

Suponhamos que desejamos demonstrar a fórmula B a partir das premissas $A_1, A_2, \cdots, A_n$, ou seja, desejamos mostrar que a fórmula B é consequência lógica das n premissas $A_1, A_2, \cdots, A_n$. Em geral, este problema se apresenta da seguinte maneira:

Demonstre: B

$$\begin{array}{cc} (1) & A_1 \\ (2) & A_2 \\ \vdots & \vdots \\ (n) & A_n \end{array}$$

As premissas foram numeradas para que possamos justificar cada passo dado. Para obtermos a linha (n + 1) na demonstração acima devemos utilizar alguma regra de inferência ou alguma equivalência lógica para justificar o passo dado. Por exemplo, se obtivermos a linha (n + 1) aplicando a regra *Modus Ponens* nas linhas (1) e (2) a nossa demonstração se torna:

Demonstre: B

$$\begin{array}{ccl} (1) & A_1 & \\ (2) & A_2 & \\ \vdots & \vdots & \\ (n) & A_n & \\ (n+1) & A_{n+1} & \text{MP } 1, 2 \end{array}$$

em que A_{n+1} é a fórmula da linha (n + 1) e MP 1, 2 significa que esta fórmula foi obtida pela aplicação da regra de inferência *Modus Ponens* nas linhas (1) e (2). Continuando assim sucessivamente, devemos construir a nossa demonstração passo a passo, justificando cada passo dado por meio de uma regra de inferência ou de uma equivalência lógica, até obtermos a fórmula B, a conclusão desejada.

Observamos que o esquema de demonstração que apresentamos nos permite verificar a validade de um argumento no qual $A_1, A_2, \cdots, A_n$ são as premissas e B é a conclusão, isto é, nos permite verificar que $A_1, A_2, \cdots, A_n \vdash B$. Este esquema é *completo e correto*, isto é, podemos provar todos os argumentos válidos, e apenas esses, nesse esquema.

Exemplos:

1) Demonstre: B

(1) $A \to B$	
(2) A	
(3) B	MP 1, 2

2) Demonstre: A

(1) $B \to A$	
(2) B	
(3) A	MP 1, 2

3) Demonstre:C

(1) $A \to B$	
(2) $(A \to B) \to C$	
(3) C	MP 1, 2

4) Demonstre: - A

(1) $A \to B$	
(2) - B	
(3) - A	MT 1, 2

5) Demonstre: $D \wedge - E$

(1) D	
(2) - E	
(3) $D \wedge - E$	A 1, 2

6) Demonstre: A

(1) $A \wedge C$	
(2) A	S 1

7) Demonstre: B

(1) $C \vee B$	
(2) - C	
(3) B	TP 1, 2

8) Demonstre: $A \vee B$

(1) A	
(2) $A \vee B$	LA 1

9) Demonstre: $A \rightarrow C$

(1) $A \rightarrow B$	
(2) $B \rightarrow C$	
(3) $A \rightarrow C$	HS 1, 2

10) Demonstre: $A \vee B$

(1) $C \vee D$	
(2) $C \rightarrow A$	
(3) $D \rightarrow B$	
(4) $A \vee B$	DS 1, 2, 3

11) Demonstre: $A \wedge B$

(1) $B \wedge A$	
(2) $A \wedge B$	CL 1

12) Demonstre: $E \vee F$

(1) $F \vee E$	
(2) $E \vee F$	CL 1

13) Demonstre: $- (R \wedge S)$

(1) $- R \vee - S$	
(2) $- (- - R \wedge - - S)$	DL 1
(3) $- (R \wedge S)$	DN 2

14) Demonstre: $A \rightarrow B$

(1) $A \leftrightarrow B$	
(2) $(A \rightarrow B) \wedge (B \rightarrow A)$	LB 1
(3) $(A \rightarrow B)$	S 2

15) Demonstre: A

(1) $B \rightarrow C$	
(2) B	
(3) $- A \rightarrow - C$	
(4) C	MP 1, 2
(5) $- - C$	DN 4
(6) $- - A$	MT 3, 5
(7) A	DN 6

Observação: As regras de inferência devem ser aplicadas exatamente como elas se apresentam. No último exemplo tínhamos:

(3) - A → - C
(4) C MP 1, 2

Para aplicarmos a regra de inferência *Modus Tollens* devemos ter a negação da fórmula - C que é - - C (e não C). Portanto, devemos antes de aplicar a regra de inferência *Modus Tollens*, aplicar a regra de inferência Dupla Negação na linha (4).

A seguir, apresentamos exercícios de fixação resolvidos com o intuito de reforçar a prática e assimilação das regras. Mas, para tanto, sugerimos que a resolução destes exercícios seja feita à parte e a resposta apresentada seja observada apenas no caso de dificuldades no processo de resolução.

1) Demonstre: - C

(1) A → - C	
(2) B → A	
(3) B	
(4) A	MP 2, 3
(5) - C	MP 1, 4

2) Demonstre: C

(1) A → B ∧ D	
(2) B ∧ D → C	
(3) A	
(4) B ∧ D	MP 1, 3
(5) C	MP 2, 4

3) Demonstre: - B

(1) C	
(2) C → - A	
(3) - A → - B	MP 1, 2
(4) - A	MP 3, 4
(5) - B	

4) Demonstre: - C

(1) A → - B	
(2) A	
(3) - B → D	
(4) D → - C	
(5) - B	MP 1,2
(6) D	MP 3, 5
(7) - C	MP 4, 6

5) Demonstre: $- - C$

(1) $B \rightarrow C$	
(2) B	
(3) C	MP 1, 2
(4) $- - C$	DN 3

6) Demonstre: $B \vee C$

(1) $A \rightarrow - - (B \vee C)$	
(2) A.	
(3) $- - (B \vee C)$	MP 1, 2
(4) $(B \vee C)$	DN 3

7) Demonstre: C

(1) $A \rightarrow B \wedge D$	
(2) A	
(3) $B \wedge D \rightarrow - - C$	
(4) $B \wedge D$	MP 1, 2
(5) $- - C$	MP 3, 4
(6) C	DN 5

8) Demonstre: $A \wedge B$

(1) $C \rightarrow - D$	
(2) D	
(3) $- C \rightarrow A \wedge B$	
(4) $- - D$	DN 2
(5) $- C$	MT 1, 4
(6) $A \wedge B$	MP 5, 3

9) Demonstre: A

(1) B	
(2) $- A \rightarrow - B$	
(3) $- - B$	DN 1
(4) $- - A$	MT 2, 3
(5) A	DN 4

10) Demonstre: $- A$

(1) $A \rightarrow B$	
(2) $B \rightarrow C$	
(3) $C \rightarrow D$	
(4) $- D$	
(5) $- C$	MT 3, 4
(6) $- B$	MT 2, 5
(7) $- A$	MT 1, 6

11) Demonstre: - B

(1) - A $\wedge$ C	
(2) B $\rightarrow$ A	
(3) - A	S 1
(4) - B	MT 2, 3

12) Demonstre: - - B

(1) A $\wedge$ B	
(2) B	S 1
(3) - - B	DN 2

13) Demonstre: - B $\wedge$ A

(1) - B $\rightarrow$ A	
(2) - (C $\wedge$ A)	
(3) B $\rightarrow$ C $\wedge$ A	
(4) - B	MT 2, 3
(5) A	MP 1, 4
(6) - B $\wedge$ A	A 4, 5

14) Demonstre: A

(1) B $\wedge$ C	
(2) C $\rightarrow$ D	
(3) B $\rightarrow$ E	
(4) D $\wedge$ E $\rightarrow$ A	
(5) B	S 1
(6) C	S 1
(7) D	MP 2, 6
(8) E	MP 3, 5
(9) D $\wedge$ E	A 7, 8
(10) A	MP 4, 9

15) Demonstre: A

(1) A $\vee$ B	
(2) - C	
(3) B $\rightarrow$ C	
(4) - B	MT 2, 3
(5) B $\vee$ A	CL 1
(6) A	TP 4, 5

16) Demonstre: $A \wedge B$

(1) B	
(2) $B \rightarrow -C$	
(3) $A \vee C$	
(4) $-C$	MP 1, 2
(5) $C \vee A$	CL 3
(6) A	TP 4, 5
(7) $A \wedge B$	A 1, 6

17) Demonstre: A

(1) $C \rightarrow A \vee B$	
(2) $- - C$	
(3) $-B$	
(4) C	DN 2
(5) $A \vee B$	MP 1, 4
(6) $B \vee A$	CL 5
(7) A	TP 3, 6

18) Demonstre: $-C$

(1) $-C \vee -A$	
(2) $- - A$	
(3) $-A \vee -C$	CL 1
(4) $-C$	TP 2, 3

19) Demonstre: $A \rightarrow B$

(1) $C \vee (A \rightarrow B)$	
(2) $-C$	
(3) $A \rightarrow B$	TP 1, 2

20) Demonstre: $A \vee -C$

(1) B	
(2) $-A \rightarrow -B$	
(3) $- - B$	DN 1
(4) $- - A$	MT 2, 3
(5) A	DN 4
(6) $A \vee -C$	LA 5

21) Demonstre: E

(1) $A \wedge -C$	
(2) $B \rightarrow C$	
(3) $B \vee D$	
(4) $D \wedge A \rightarrow E$	
(5) $-C$	S 1
(6) A	S 1

(7) $-B$	MT 2, 5
(8) D	TP 3, 7
(9) $D \wedge A$	A 6, 8
(10) E	MP 4, 9

22) Demonstre: B

(1) $-A$	
(2) $-B \rightarrow C$	
(3) $C \rightarrow A$	
(4) $-C$	MT 1, 3
(5) $- - B$	MT 2, 4
(6) B	DN 5

23) Demonstre: - C

(1) $-D \rightarrow E \vee A$	
(2) $E \vee A \rightarrow -C$	
(3) $-A \rightarrow -B$	
(4) B	
(5) $A \rightarrow -D$	
(6) $-D \rightarrow -C$	HS 1, 2
(7) $- - B$	DN 4
(8) $- - A$	MT 3, 7
(9) A	N 8
(10) $-D$	MP 5, 9
(11) $-C$	MP 6, 10

24) Demonstre: C

(1) $D \vee -A$	
(2) $-A \rightarrow B$	
(3) $D \rightarrow C$	
(4) $-B$	
(5) $- - A$	MT 2, 4
(6) $-A \vee D$	CL 1
(7) D	TP 5, 6
(8) C	MP 3, 7

25) Demonstre: - D ∧ B

(1) $B \wedge -A$	
(2) $A \vee -C$	
(3) $D \rightarrow C$	
(4) B	S 1
(5) $-A$	S 1
(6) $-C$	TP 2, 5
(7) $-D$	MT 3, 6
(8) $-D \wedge B$	A 4, 7

26) Demonstre: $- A \vee B$

(1) $- C \vee D$	
(2) $- C \rightarrow - A$	
(3) $D \rightarrow B$	
(4) $- A \vee B$	DS 1, 2, 3

27) Demonstre: A

(1) $A \vee B$	
(2) $B \rightarrow C$	
(3) $- C$	
(4) $- B$	MT 2, 3
(5) $B \vee A$	CL 1
(6) A	TP 4, 5

28) Demonstre: $B \wedge D$

(1) $A \vee C$	
(2) $- C$	
(3) $A \rightarrow D \wedge B$	
(4) $C \vee A$	CL 1
(5) A	TP 2, 4
(6) $D \wedge B$	MP 3, 5
(7) $B \wedge D$	CL 6

29) Demonstre: $B \wedge A$

(1) $(A \wedge B) \vee D$	
(2) $E \rightarrow - D$	
(3) $C \rightarrow - D$	
(4) $E \vee C$	
(5) $- D \vee - D$	DS 2, 3, 4
(6) $- D$	LI 5
(7) $D \vee (A \wedge B)$	CL 1
(8) $A \wedge B$	TP 6, 7
(9) $B \wedge A$	CL 8

30) Demonstre: C

(1) $D \rightarrow E$	
(2) $E \rightarrow A$	
(3) $(D \rightarrow A) \rightarrow - B$	
(4) $B \vee C$	
(5) $D \rightarrow A$	HS 1, 2
(6) $- B$	MP 3, 5
(7) C	TP 4, 6

31) Demonstre: - B

(1) - (A $\wedge$ D)	
(2) - D $\rightarrow$ C	
(3) - A $\rightarrow$ C	
(4) B $\rightarrow$ - C	
(5) - A $\vee$ - D	DL 1
(6) C $\vee$ C	DS 2, 3, 5
(7) C	LI 6
(8) - - C	DN 7
(9) - B	MT 4, 8

32) Demonstre: A $\wedge$ E

(1) - B $\rightarrow$ - (D $\vee$ - C)	
(2) C $\rightarrow$ E $\wedge$ A	
(3) - B	
(4) - (D $\vee$ - C)	MP 1, 3
(5) - D $\wedge$ - - C	DL 4
(6) - - C	S 5
(7) C	DN 6
(8) E $\wedge$ A	MP 2, 7
(9) A $\wedge$ E	CL 8

33) Demonstre: D

(1) - A $\rightarrow$ B	
(2) C $\rightarrow$ B	
(3) C $\vee$ - A	
(4) - B $\vee$ D	
(5) B $\vee$ B	DS 1, 2, 3
(6) B	LI 5
(7) - - B	DN 6
(8) D	TP 4, 7

34) Demonstre: - D

(1) A $\rightarrow$ - D	
(2) (A $\wedge$ B) $\vee$ C	
(3) C $\rightarrow$ (E $\vee$ F)	
(4) - E $\wedge$ - F	
(5) - (- - E $\vee$ - - F)	DL 4
(6) - (E $\vee$ F)	DN 5
(7) - C	MT 3, 6
(8) C $\vee$ (A $\wedge$ B)	CL 2
(9) A $\wedge$ B	TP 7, 8
(10) A	S 9
(11) - D	MP 1, 10

35) Demonstre: $A \vee - B$

(1) $E \vee F \rightarrow - B$	
(2) $C \rightarrow E$	
(3) $D \rightarrow F$	
(4) $C \vee D$	
(5) $E \vee F$	DS 2, 3, 4
(6) $- B$	MP 1, 5
(7) $- B \vee A$	LA 6
(8) $A \vee - B$	CL 7

36) Demonstre: $C \vee B$

(1) $C \leftrightarrow D$	
(2) $D \vee A$	
(3) $A \rightarrow B$	
(4) $(C \rightarrow D) \wedge (D \rightarrow C)$	LB 1
(5) $D \rightarrow C$	S 4
(6) $C \vee B$	DS 2, 3, 5

37) Demonstre: $B \rightarrow A$

(1) $C \leftrightarrow B$	
(2) $C \rightarrow A$	
(3) $(C \rightarrow B) \wedge (B \rightarrow C)$	LB 1
(3) $B \rightarrow C$	S 3
(4) $B \rightarrow A$	HS 2, 4

38) Demonstre: $- (- A \wedge - B)$

(1) $C \leftrightarrow B$	
(2) $A \leftrightarrow A$	
(3) $C \vee A$	
(4) $(C \rightarrow B) \wedge (B \rightarrow C)$	LB 1
(5) $(A \rightarrow A) \wedge (A \rightarrow A)$	LB 1
(6) $C \rightarrow B$	S 4
(7) $A \rightarrow A$	S 5
(8) $B \vee A$	DS 3, 6, 7
(9) $A \vee B$	CL 8
(10) $- (- A \wedge - B)$	DL 9

39) Demonstre: $- (A \wedge B)$

(1) $A \rightarrow - A$	
(2) $B \leftrightarrow - A$	
(3) $C \vee D \rightarrow B$	
(4) $(A \rightarrow B) \rightarrow C$	
(5) $(B \rightarrow - A) \wedge (- A \rightarrow B)$	LB 1
(6) $- A \rightarrow B$	S 5
(7) $A \rightarrow B$	HS 1, 6

(8) C	MP 4, 7
(9) $C \vee D$	LA 8
(10) B	MP 3, 9
(11) $B \rightarrow - A$	S 5
(12) - A	MP 10, 11
(13) $- A \vee - B$	LA 12
(14) $- (A \wedge B)$	DL 13

Já observamos anteriormente que as regras de inferência devem ser aplicadas exatamente como elas se apresentam. No entanto é comum observar tentativas de aplicá-las utilizando como premissa uma subfórmula desta, ou seja, utilizando apenas uma parte de alguma premissa. Esta é uma prática que não aconselhamos, pois, por exemplo, se aplicamos erroneamente a Simplificação à fórmula $- (A \wedge B)$ obtendo como conclusão - A ou - B temos que qualquer uma destas não é consequência lógica de $- (A \wedge B)$, conforme mostra a tabela a seguir:

A	B	$A \wedge B$	$- (A \wedge B)$	- A	- B
V	V	V	F	F	F
V	F	F	V	F	V
F	V	F	V	V	F
F	F	F	V	V	V

Por outro lado, aplicando *Modus Ponens* às premissas A e $- (A \rightarrow B)$ para obter como conclusão - B, temos que - B é consequência lógica de A e $- (A \rightarrow B)$, como mostra a tabela abaixo:

A	B	$A \rightarrow B$	$- (A \rightarrow B)$	- B
V	V	V	F	F
V	F	F	V	V
F	V	V	F	F
F	F	V	F	V

O mesmo acontece com muitas outras situações, como por exemplo, aplicando a regra *Modus Ponens* às premissas A e

$(A \rightarrow B) \wedge C$ para concluir $B \wedge C$, e então poderíamos ter muitas outras regras de inferência. Mas veja que estas novas regras são desnecessárias, ou na verdade não são novas, elas resultam da aplicação de regras já conhecidas. No exemplo dado, a partir das premissas A e $(A \rightarrow B) \wedge C$ aplicando as regras Simplificação, *Modus Ponens* e Adjunção, obtemos a conclusão desejada $B \wedge C$.

Por isso, reafirmamos que as regras de inferência devem ser aplicadas exatamente como elas se apresentam e não devemos aplicá-las a partes de premissas.

4.1 Consistência e inconsistência

Definição: Diremos que um conjunto de fórmulas é *consistente* se existir uma atribuição de valores verdade feita às variáveis proposicionais das fórmulas desse conjunto, de modo que os valores lógicos das fórmulas desse conjunto sejam simultaneamente verdadeiros (V). Caso contrário diremos que esse conjunto é *inconsistente*.

Exemplo: Consideremos o seguinte conjunto de fórmulas:

(1) $p \wedge - q$
(2) $- (r \vee q)$
(3) $p \rightarrow p_0$

Observe que, fazendo vl(p) = V, vl(q) = F, vl(r) = F, e vl(p_0) = V, teremos vl($p \wedge - q$) = V, vl($- (r \vee q)$) = V, e vl($p \rightarrow p_0$) = V. Assim, o conjunto de fórmulas deste exemplo é consistente.

Exemplo: Consideremos o seguinte conjunto de fórmulas:

(1) $- q \rightarrow r$
(2) $- r \vee r_1$
(3) $- (p \vee q)$
(4) $- p \rightarrow - r_1$

Observe que para que tenhamos vl($- (p \vee q)$) = V a única atribuição que nos serve é vl(p) = vl(q) = F. Assim, para que tenhamos vl($- q \rightarrow r$) = V, devemos exigir unicamente que vl(r) = V e também que vl(r_1) = F. Mas, desta forma, temos vl($- r \vee r_1$) = F. Portanto, não existe atribuição de valores verdade feita às variáveis proposicionais dessas fórmulas de modo que os valores lógicos delas sejam simultaneamente verdadeiros (V). Logo, o conjunto é inconsistente.

Veja que se $A_1, A_2, \cdots, A_n$ é um conjunto inconsistente, a regra de inferência Adjunção nos permite concluir que $A_1 \wedge A_2 \wedge \cdots \wedge A_n$ é uma contradição. Isto nos conduz à seguinte definição.

Definição: Diremos que um conjunto de fórmulas é *inconsistente* se dele deduzirmos uma contradição, isto é, se através do uso de regras de inferência pudermos, a partir desse conjunto de fórmulas, chegar a uma contradição. Observe que toda fórmula que é uma contradição é logicamente equivalente a uma fórmula do tipo $A \wedge - A$, em que A é uma fórmula.

Exemplos:

1) Consideremos o seguinte conjunto de fórmulas:

(1) $- q \rightarrow r$
(2) $- r \vee r_1$
(3) $- (p \vee q)$
(4) $- p \rightarrow - r_1$

Vamos mostrar que este conjunto de fórmulas é inconsistente.

(1) $- q \rightarrow r$	
(2) $- r \vee r_1$	
(3) $- (p \vee q)$	
(4) $- p \rightarrow - r_1$	
(5) $- p \wedge - q$	DL 3
(6) $- q$	S 5
(7) r	MP 1, 6
(8) $- p$	S 5
(9) $- r_1$	MP 4, 8
(10) $r_1 \vee - r$	CL 2
(11) $- r$	TP 9, 10
(12) $r \wedge - r$	A 7, 11

A linha (12) caracteriza uma contradição, pois é uma fórmula do tipo $A \wedge - A$, em que agora A é a fórmula r. Portanto, o conjunto de fórmulas deste exemplo é inconsistente.

2) O conjunto de fórmulas:

(1) $p \rightarrow q$
(2) $q \rightarrow r$

$$(3)\ - r \vee r_1$$

é consistente, pois se tomarmos vl(p) = V, vl(q) = V, vl(r) = V e vl(r_1) = V temos vl($p \to q$) = V, vl($q \to r$) = V e vl($- r \vee r_1$) = V.

3) O conjunto de fórmulas

$$(1)\ p_1 \to p$$
$$(2)\ p_1 \wedge r$$
$$(3)\ q \to - r$$
$$(4)\ p \vee r_1 \to q$$

é inconsistente, pois pela demonstração:

(5) p_1	S 2
(6) r	S 2
(7) $- - r$	DN 6
(8) $- q$	MT 3, 7
(9) $- (p \vee r_1)$	MT 4, 8
(10) $- p \wedge - r_1$	DL 9
(11) $- p$	S 10
(12) $p \wedge - p$	A 5, 11

obtemos a contradição $p \wedge - p$.

As definições dadas ainda valem se o conjunto de fórmulas em questão for formado por apenas uma fórmula.

Observe que de um conjunto de fórmulas inconsistente podemos deduzir qualquer fórmula, pois a partir de um conjunto de fórmulas inconsistente, em uma certa linha (i), obtemos uma contradição do tipo:

$$A \wedge - A,$$

em que A é uma fórmula.

Continuando a aplicação de regras de inferência podemos obter:

(i)	$A \wedge - A$	
(i + 1)	A	S i
(i + 2)	$A \vee B$	LA i + 1
(i + 3)	$- A$	S i
(i + 4)	B	TP i + 2, i + 3

Portanto, concluímos a fórmula “B” a partir da fórmula “$A \wedge - A$”. Lembramos que como “B” representa uma fórmula qualquer, podemos concluir qualquer fórmula a partir da fórmula $A \wedge - A$.

Observações:

1) Obtendo-se, através de uma demonstração, uma conclusão a partir de um conjunto de premissas ou hipóteses consistente, o valor lógico dessa conclusão será verdadeiro (V) sempre que os valores lógicos das premissas forem simultaneamente verdadeiros (V), pois a conclusão é consequência lógica das premissas.

2) Utilizando a regra de inferência Lei da Adição a partir de uma premissa A, podemos concluir $A \vee B$ em que B é uma fórmula qualquer, podendo ser inclusive uma contradição. No entanto, desde que o conjunto de premissas seja consistente, nenhuma demonstração nos permitirá concluir B, pois, como já dissemos, a conclusão será consequência lógica das premissas.

3) Quando dizemos que um conjunto de fórmulas $A_1, A_2, \cdots, A_n$ não é consistente, ou seja, que não existe nenhuma atribuição de valores de verdade feita às variáveis proposicionais das fórmulas $A_1, A_2, \cdots, A_n$ tal que os valores lógicos das fórmulas $A_1, A_2, \cdots, A_n$ sejam todos simultaneamente verdadeiros (V), equivale a dizer que o conjunto de fórmulas $A_1, A_2, \cdots, A_n$ é inconsistente, pois a partir das premissas $A_1, A_2, \cdots, A_n$, usando a regra de inferência Adjunção (A), podemos chegar a seguinte conclusão:

$$A_1 \wedge A_2 \wedge \cdots \wedge A_n,$$

que é uma contradição.

4) Quando dizemos que um conjunto de fórmulas $A_1, A_2, \cdots, A_n$ não é inconsistente, isto é, usando regras de inferência não conseguimos deduzir dele uma contradição, então este conjunto de fórmulas é consistente. Suponhamos por absurdo, que ele não é consistente, ou seja, que não existe uma atribuição de valores verdade feita às variáveis proposicionais de $A_1, A_2, \cdots, A_n$ tal que os valores lógicos dessas fórmulas simultaneamente verdadeiros (V). Assim, usando a regra de inferência Adjunção (A), obtemos a contradição $A_1 \wedge A_2 \wedge \cdots \wedge A_n$, o que é um absurdo pois $A_1, A_2, \cdots, A_n$ não é inconsistente. Logo $A_1, A_2, \cdots, A_n$ é consistente.

4.2 Método dedutivo

Quando no argumento $A_1, A_2, \cdots, A_n \vdash B$ a conclusão B é uma formula do tipo condicional, isto é, B é do tipo $(R \rightarrow S)$ em que R e S são fórmulas quaisquer, o nosso argumento torna-se:

$$A_1, A_2, \cdots, A_n \vdash R \rightarrow S.$$

O método dedutivo nos permite adicionar R como premissa para depois demonstrar S, e daí o nosso argumento torna-se:

$$A_1, A_2, \cdots, A_n, R \vdash S.$$

Isso é uma vantagem, pois nos dá uma hipótese a mais. Este método está baseado no Teorema da Dedução.

Teorema da dedução: Se Γ é um conjunto de fórmulas, A e B são fórmulas e Γ, A $\vdash$ B, então $\Gamma \vdash (A \to B)$. Em particular, se A $\vdash$ B, então $\vdash (A \to B)$.

Demonstração:

Para isto, suponha que Γ, A $\vdash$ B e que Γ não implica logicamente $(A \to B)$. Assim existe pelo menos uma atribuição de valores verdade feita às variáveis proposicionais das fórmulas de Γ e de A e B, tal que para essa atribuição temos que as fórmulas de Γ assumem simultaneamente o valor lógico verdadeiro e o valor lógico de $(A \to B)$ é falso. Mas daí teremos vl(A) = V e vl(B) = F, contradizendo o fato de Γ, A $\vdash$ B.

Exemplo: Use o método dedutivo para provar que $(A \to (A \to B)) \vdash (A \to B)$:

Pelo método dedutivo para isto é suficiente provar que $(A \to (A \to B)), A \vdash B$, cuja validade é provada através da seguinte demonstração:

Demonstre: B

(1) $(A \to (A \to B))$	
(2) A	
(3) $A \to B$	MP 1,2
(4) B	MP 2,3

Veja a seguir uma demonstração para o argumento dado sem utilizar o método dedutivo e observe o quanto este método facilita a demonstração.

Demonstre: $A \to B$

(1) $(A \to (A \to B))$	
(2) $(- A \vee (A \to B))$	LC 1
(3) $- (A \wedge - (A \to B))$	DL 2
(4) $- (A \wedge - (- A \vee B))$	LC 3
(5) $- (A \wedge (A \wedge - B))$	DL 4

(6) $-((A \wedge A) \wedge - B)$	AL 5
(7) $-(A \wedge - B)$	LI 6
(8) $(- A \vee B)$	DL 7
(9) $(A \rightarrow B)$	LC 8

4.3 Argumentos verbais

Na apresentação deste livro esclarecemos que nesta obra não temos a preocupação com contextualizações, pois para tanto seria necessário escolher uma específica área para a aplicação da Lógica Matemática. No entanto, neste tópico abordaremos muito brevemente a argumentação contextualizada, aplicando o que até agora estudamos com o objetivo de testar logicamente a validade da argumentação.

Lembramos que um argumento é válido se e somente se a conclusão é consequência lógica da(s) premissa(s), ou seja, se existe uma demonstração deste argumento. Assim, dado um argumento em português, formado por proposições, agora chamadas de declarações, para testá-lo logicamente realizamos as duas seguintes etapas:

1. Simbolizamos cada declaração usando as fórmulas do Cálculo Proposicional.
2. Construímos uma sequência de demonstração utilizando as regras de inferência ou as equivalências lógicas.

A seguir apresentaremos um exemplo, sem vínculo algum com os cursos para os quais esta obra destina-se, para que a compreensão não esteja vinculada ao conhecimento de conceitos específicos.

Exemplo: Considere o argumento "Se as taxas de juros caírem o mercado imobiliário vai melhorar. O Imposto sobre Operações Financeiras - IOF vai diminuir ou o mercado imobiliário não vai melhorar. As taxas de juros vão cair. Portanto, o IOF vai diminuir.". Usando a notação:

J: a taxa de juros vai cair;

I: o mercado imobiliário vai melhorar; e

F: o IOF vai diminuir,

o argumento fica: $(J \to I) \wedge (F \vee - I) \wedge J \vdash F$, cuja validade é testada demonstrando-o, ou seja:

Demonstre: F

(1) $J \to I$	
(2) $F \vee - I$	
(3) J	
(4) I	MP 1, 3
(5) $- - I$	DN4
(6) $- I \vee F$	CL 2
(7) F	TP 5, 6

Na verdade, uma prática interessante é adaptar exemplos ou exercícios sobre demonstrações apresentados neste capítulo como uma argumentação verbal da sua área. Por exemplo, considerando o oitavo exercício do bloco de exercícios para fixação deste capítulo:

Demonstre: $A \wedge B$

(1) $C \to - D$
(2) D
(3) $- C \to A \wedge B$

um estudante de Ciência da Computação, para adaptá-lo como um argumento verbal, pode supor que:

A: ser demitido;
B: passar necessidades;
C: software ter bom desempenho; e
D: ser advertido.

Assim, o argumento verbal será: "Se o software tiver bom desempenho então não serei advertido. Fui advertido. Se o software não tiver bom desempenho então serei demitido e passarei necessidades. Portanto, serei demitido e passarei necessidades".

Veja então que esse argumento é válido, pois já o demonstramos ao resolver o citado exercício.

Observe que se esse estudante pode supor que:

A: ser promovido;
B: receber gratificação;
C: software ter bom desempenho; e
D: ser advertido.

Daí argumento verbal será: "Se o software tiver bom desempenho então não serei advertido. Fui advertido. Se o software não tiver bom desempenho então serei promovido e receberei gratificação. Portanto, serei promovido e receberei gratificação".

Veja então que este argumento também é válido do ponto de vista da Lógica Matemática, pois já o demonstramos ao resolver o citado exercício, mas, é claro, há alguma coisa errada. Esta validade é uma função apenas do formato lógico do argumento e não tem nada a ver com a verdade fatual de nenhum de seus componentes.

Por isso deixaremos o estudo dos argumentos verbais aos diretamente envolvidos com os fatos nele relacionados, mas temos certeza que neste momento o nosso leitor possui habilidade suficiente para analisar a validade do formato lógico de qualquer argumento.

4.4 Exercícios propostos

1) Nas demonstrações a seguir, justifique os passos em negrito:

a) Demonstre: A

(1) - B → - C
(2) - B
(3) - C → A
(4) - C
(5) A

b) Demonstre: C

(1) - B
(2) A → B
(3) - A → C
(4) - A
(5) C

c) Demonstre: - A

(1) A → - C
(2) B → C
(3) B

(4) C
(5) - - C
(6) - A

d) Demonstre: B $\wedge$ A
(1) B $\wedge$ C
(2) B $\rightarrow$ A
(3) B
(4) A
(5) B $\wedge$ A

e) Demonstre: A
(1) C $\wedge$ D
(2) A $\vee$ - B
(3) C $\rightarrow$ B
(4) C
(5) B
(6) - - B
(7) - B $\vee$ A
(8) A

f) Demonstre: C $\wedge$ (A $\vee$ B)
(1) A $\vee$ B
(2) B $\rightarrow$ C
(3) A $\rightarrow$ C
(5) C $\vee$ C
(6) C
(7) C $\wedge$ (A $\vee$ B)

g) Demonstre: D
(1) A $\rightarrow$ B
(2) B $\rightarrow$ - C
(3) C
(4) A $\vee$ (E $\wedge$ D)
(5) A $\rightarrow$ - C
(6) - - C

(7) - A
(8) E $\wedge$ D
(9) D $\wedge$ E
(10) D

h) Demonstre: - A $\wedge$ - B
(1) - C $\leftrightarrow$ B $\vee$ A
(2) - (D $\vee$ - C)
(3) - D $\wedge$ - - C
(4) - - C
(5) B $\vee$ A $\rightarrow$ - C
(6) - (B $\vee$ A)
(7) - B $\wedge$ - A
(8) - A $\wedge$ - B

2) Demonstre: B $\vee$ C
(1) - A $\rightarrow$ B $\vee$ C
(2) F $\vee$ G $\rightarrow$ - A
(3) F $\vee$ G

3) Demonstre: B
(1) - G $\rightarrow$ E
(2) E $\rightarrow$ A
(3) - G
(4) A $\rightarrow$ - C
(5) - C $\rightarrow$ D
(6) D $\rightarrow$ B

4) Demonstre: E $\vee$ G
(1) C $\vee$ D
(2) C $\vee$ D $\rightarrow$ - F
(3) - F $\rightarrow$ A $\wedge$ - B
(4) A $\wedge$ - B $\rightarrow$ E $\vee$ G

5) Demonstre: B
(1) - A
(2) - A $\rightarrow$ - - B

6) Demonstre: - - B

(1) A $\rightarrow$ - C

(2) - C $\rightarrow$ B

(3) A.

7) Demonstre: A

(1) B $\rightarrow$ C

(2) - B $\rightarrow$ - - A

(3) - C

8) Demonstre: - D

(1) A $\rightarrow$ B

(2) B $\rightarrow$ C

(3) D $\rightarrow$ - C

(4) A

9) Demonstre: A $\wedge$ B

(1) C $\rightarrow$ A

(2) C

(3) C $\rightarrow$ B

10) Demonstre: A $\wedge$ C

(1) A $\wedge$ - B

(2) - C $\rightarrow$ B

11) Demonstre: B

(1) - A $\vee$ B

(2) - A $\rightarrow$ C

(3) - C

12) Demonstre: B

(1) - C

(2) C $\vee$ (B $\vee$ A)

(3) - A

13) Demonstre: B
(1) $- A \vee C$
(2) $- C$
(3) $- (B \wedge C) \rightarrow A$

14) Demonstre: $- A$
(1) $- A \vee B$
(2) $- B$

15) Demonstre: $D \vee C$
(1) $A \vee C$
(2) $A \rightarrow B$
(3) $- B$

16) Demonstre: $B \vee - C$
(1) $C \wedge A$
(2) $D \rightarrow - A$
(3) $- D \rightarrow B$

17) Demonstre: $- C$
(1) $(B \rightarrow C) \wedge A$
(2) $C \rightarrow D$
(3) $(B \rightarrow C) \rightarrow - D$

18) Demonstre: B
(1) $- C \rightarrow D$
(2) $C \rightarrow A \wedge B$
(3) $D \rightarrow E$
(4) $- E$

19) Demonstre: $- D \wedge - A$
(1) $- C \vee - B$
(2) $- B \rightarrow - D$
(3) $- C \rightarrow A$
(4) $- A$

20) Demonstre: $C \vee D$
(1) $- A \vee - B$
(2) $- A \rightarrow C$
(3) $- B \rightarrow D$

21) Demonstre: $- A \wedge B$
(1) $A \rightarrow C$
(2) $- C \wedge - D$
(3) $- D \rightarrow B$

22) Demonstre: $- (C \wedge - E)$
(1) $(C \wedge - E) \rightarrow - D$
(2) $A \rightarrow D$
(3) $A \wedge B$

23) Demonstre: $B \vee D$
(1) $A \rightarrow B$
(2) $A \vee C$
(3) $- C$

24) Demonstre: $- A$
(1) $C \rightarrow E$
(2) $D \rightarrow B$
(3) $E \vee B \rightarrow - A$
(4) $C \vee D$

25) Demonstre: $- (A \vee B)$
(1) $C \wedge - D$
(2) $C \rightarrow - A$
(3) $D \vee - B$

26) Demonstre: $- C$
(1) $A \rightarrow - B$
(2) $- B \rightarrow - D$
(3) $(A \rightarrow - D) \rightarrow -E$
(4) $C \rightarrow E$

27) Demonstre: $- E$

(1) $E \rightarrow A \wedge D$
(2) $B \rightarrow - A$
(3) $C \rightarrow - D$
(4) $C \vee B$

28) Demonstre: $E \wedge B$

(1) $A \vee B$
(2) $D \rightarrow B \wedge E$
(3) $A \rightarrow D$
(4) $B \rightarrow D$

29) Demonstre: $- A$

(1) $A \leftrightarrow B$
(2) $- C$
(3) $B \rightarrow C$

30) Demonstre: $A \vee C$

(1) $A \leftrightarrow B$
(2) $B \wedge D$

31) Demonstre: $A \leftrightarrow B$

(1) $B \leftrightarrow C$
(2) $C \leftrightarrow A$

32) Verifique, em cada item, se o conjunto de fórmula dado é consistente ou inconsistente:

a) (1) $p \rightarrow r$
(2) $- r \rightarrow p_1$
(3) $p_1 \vee p$

b) (1) $- p \vee - r$
(2) $- p \rightarrow r_1$
(3) $- r_1$

c) (1) $r \rightarrow r \wedge q$
(2) $- r_1 \vee r$
(3) $- p_1 \vee - q$
(4) $r_1 \wedge p_1$

d) (1) $r \to q$
(2) $p \to q$
(3) $q \to - p_1$

e) (1) $p_1 \vee - r$
(2) $- (- r \vee r_1)$
(3) $p_1 \to r_1$

33) Use o método dedutivo para provar a validade do argumento $(A \to B), (B \to C) \vdash (A \to C)$, ou seja, a regra de inferência Silogismo Hipotético.

5

Cálculo de Quantificadores

No Cálculo Proposicional, simbolizamos as proposições por meio de letras, as analisamos, as comparamos e inferimos a partir de um conjunto destas proposições. No entanto, existem frases como por exemplo:

Todos os cavalos;

Alguns cavalos;

Todos os alunos são inteligentes;

Nenhum carro é branco;

Algum cavalo é branco;

entre outras, as quais frequentemente figuram nos mais diversos raciocínios e exigem outras regras além das já estudadas.

O estudo deste tipo de expressão recebe o nome de *Cálculo de Quantificadores* ou *Cálculo de Predicados*, fundamento para a Inteligência Artificial, importante objeto de estudo na Ciência da Computação.

Quantificar significa determinar a quantidade. Assim, Cálculo de Quantificadores significa calcular com variáveis que representam quantidades. Por exemplo, na expressão “todo número par é divisível por 2" a palavra "todo" está significando que a quantidade de todos os números pares que são divisíveis por 2. Cabe ressaltar que quantidades específicas não são importantes, pois podem ser tratadas simplesmente como todos elementos ou como parte do todo, ou seja como alguns elementos, dependendo da totalidade a se considerar.

Assim, existem dois tipos de quantificadores: O primeiro é o *quantificador universal*, que tratará das expressões que envolvem a totalidade de um universo ou domínio, ou seja expressões do tipo *"para todo"*, *"para cada"* ou *"para qualquer"* e seus sinônimos ou plurais, e será representado pelo símbolo $\forall$, para então $\forall(x)$ representar as expressões "todo x", "cada x" ou "qualquer x" e seus sinônimos ou plurais. E o segundo é o *quantificador existencial*, que tratará das expressões que envolvem uma parte de um universo ou domínio, ou seja expressões do tipo *"existe"*, *"existe pelo menos um"* ou *"para algum"* e seus sinônimos ou plurais, e será representado pelo símbolo $\exists$, para então $\exists(x)$ representar as expressões "algum x" ou "existe x" e seus sinônimos ou plurais.

O universo ou domínio descrito é o conjunto no qual estamos trabalhando, e é de fundamental importância, pois uma mesma expressão do Cálculo de Quantificadores pode ser verdadeira em um determinado domínio e falso em outro domínio. Por exemplo, a expressão "algum aluno tem menos de 10 anos" é falsa se considerarmos como universo o conjunto formado por todos alunos do Ensino Superior, mas será verdadeira se considerarmos como universo o conjunto formado pelos alunos da Educação Básica. Atentamos para o fato de que este nosso estudo somente será significativo se o domínio a considerar incluir pelo menos um objeto, e assim admitiremos todos os universos deste capítulo.

Para formalizarmos a expressão "para todo x, x > 0" devemos escrever:

$$\forall(x)(x > 0),$$

e para formalizarmos a expressão "existe x > 0" devemos escrever:

$$\exists(x)(x > 0).$$

Para formalizarmos as expressões "todos os cavalos" ou "alguns cavalos", precisamos representar a propriedade "ser cavalo", o que fazemos definindo um predicado utilizando letras maiúsculas do alfabeto, por exemplo, C. Assim, se C representa a propriedade "ser cavalo", o que denotamos por:

C: ser cavalo,

C(x) representará "x é um cavalo" e:

$$\forall(x)C(x)$$

significará "todos os cavalos" e:

$$\exists(x)C(x)$$

significará "alguns cavalos".

De maneira geral, se P representa uma propriedade, o *predicado* P(x) representará que "x possui a propriedade P" e $\forall(x)P(x)$ representará "todo x que possui a propriedade P", ou ainda "todos que possuem a propriedade P" e suas variações na Língua Portuguesa, o que chamaremos de *universalização*. Da mesma forma, $\exists(x)P(x)$ representará "existe x com a propriedade P" ou ainda "alguns que possuem a propriedade P" e suas variações na Língua Portuguesa, o que chamaremos de *particularização*.

Destacamos que a negação de $\forall(x)P(x)$, isto é, $-(\forall(x)P(x))$ é $\exists(x)(-P(x))$, ou seja, dizer que "é falso que todo x possui a propriedade P" significa dizer que "algum x não possui a propriedade P". A negação de $\exists(x)P(x)$, isto é, $-(\exists(x)P(x))$ é $\forall(x)(-P(x))$, isto é, dizer que "é falso que existe x que possui a propriedade P" significa dizer que "todo x não possui a propriedade P".

5.1 Afirmativa universal, negativa universal, afirmativa particular, negativa particular e suas negações

Para formalizar a frase "todo número par é divisível por 2", seja P representando a propriedade "ser um número par", para P(x) representar "x é um número par" e seja Q representando a propriedade "ser divisível por 2", para Q(x) representar "x é divisível por 2". Daí $\forall(x)P(x)$ representará "todo x, tal que x é um número par", e usando o que foi estudado no Cálculo Proposicional, podemos definir formalmente a frase toda:

$$\forall(x)(P(x) \rightarrow Q(x)),$$

que representará "todo x, se x é um número par então x é divisível por 2", em outras palavras, "todo número x que é par é divisível por 2" ou ainda, "todo número par é divisível por 2".

Em geral, toda expressão do tipo "todo A é B" (ou "todos A são B") é formalizada por:

$$\forall(x)(A(x) \rightarrow B(x)),$$

em que A e B representam propriedades. As expressões desta forma são chamadas de *afirmativas universais*.

Observe que, se P representa uma propriedade qualquer, então P(x) formaliza "x possui a propriedade P". Assim - P(x) formalizará "x não possui a propriedade P".

Consideremos agora a frase "nenhum político é honesto" e seja A representando a propriedade "ser político", para A(x) representar "x é um político" e seja B representando a propriedade "ser honesto" para B(x) representar "x é honesto". Daí, $\forall(x)(A(x) \rightarrow - B(x))$ representará "todo x, se x é político então x não é honesto", ou ainda "todo político não é honesto", que é o mesmo que "nenhum político é honesto".

Em geral, toda expressão do tipo "nenhum A é B" (ou "todos A não são B") é formalizada por:

$$\forall(x)(A(x) \rightarrow - B(x)),$$

em que A e B representam propriedades. As expressões desta forma são chamadas de *negativas universais*.

Consideremos agora a frase "algum político é honesto" e seja A representando a propriedade "ser político", para A(x) representar "x é um político" e seja B representando a propriedade "ser honesto" para B(x) representar "x é honesto". Daí, usando o que foi estudado no Cálculo Proposicional, $\exists(x)(A(x) \wedge B(x))$ representará "existe x, tal que x é político e x é honesto", ou ainda "existe alguém que é político e é honesto", que é o mesmo que "algum político é honesto".

Em geral, toda expressão do tipo "algum A é B" (ou "alguns A são B") é formalizada por:

$$\exists(x)(A(x) \wedge B(x)),$$

em que A e B representam propriedades. As expressões desta forma são chamadas de *afirmativas particulares*.

Consideremos agora a frase “algum político não é honesto” e seja A representando a propriedade “ser político” para A(x) representar “x é um político” e seja B representando a propriedade “ser honesto” para B(x) representar “x é honesto”. Daí, $\exists(x)(A(x) \wedge - B(x))$ representará “existe x, tal que x é político e x não é honesto”, ou ainda “existe alguém que é político e é honesto”, que é o mesmo que “algum político não é honesto”.

Em geral, toda expressão do tipo “algum A não é B” (ou “alguns A não são B”) é formalizada por:

$$\exists(x)(A(x) \wedge - B(x)),$$

em que A e B representam propriedades. As expressões desta forma são chamadas de *negativas particulares*.

Resumindo, se A e B representam propriedades quaisquer, os quatro casos anteriores são:

Afirmativa universal: Todo A é B (ou todos A são B) que é representada por:

$$\forall(x)(A(x) \rightarrow B(x)).$$

Negativa universal: Nenhum A é B (ou todos A não são B) que é representada por:

$$\forall(x)(A(x) \rightarrow - B(x)).$$

Afirmativa particular: Algum A é B (ou alguns A são B) que é representada por:

$$\exists(x)(A(x) \wedge B(x)).$$

Negativa particular: Algum A não é B (ou alguns A não são B) que é representada por:

$$\exists(x)(A(x) \wedge - B(x)).$$

Destacamos que a negação da afirmativa universal, todo A é B, é nem todo A é B, ou ainda, algum A não é B, ou seja, a negativa particular. Quando negamos negativa universal, nenhum A é B, estamos dizendo que é falso que nenhum A é B, e assim, algum A é B, ou seja a negação da negativa universal é a afirmativa particular. A negação da afirmativa particular, algum A é B, que é nenhum A é B, é a negativa universal. Por fim, a negação da negativa particular, algum A não é B, significa que todo A é B, ou seja, é a afirmativa universal.

Simbolicamente:

$- (\forall(x)(A(x) \rightarrow B(x)))$ é o mesmo que $\exists(x)(A(x) \wedge - B(x))$;
$- (\forall(x)(A(x) \rightarrow - B(x)))$ é o mesmo que $\exists(x)(A(x) \wedge B(x))$;
$- (\exists(x)(A(x) \wedge B(x)))$ é o mesmo que $\forall(x)(A(x) \rightarrow - B(x))$; e
$- (\exists(x)(A(x) \wedge - B(x)))$ é o mesmo que $\forall(x)(A(x) \rightarrow B(x))$.

5.2 Formalização

Para formalizar expressões do Cálculo de Quantificadores, necessitamos em primeiro lugar definir os predicados que representam as propriedades, as variáveis e as constantes envolvidas. Os predicados são representadas por letras maiúsculas do alfabeto. Conforme já determinamos, as classes de elementos serão representadas pelas *variáveis* $x, x_0, x_1, \cdots$ e para formalizar um elemento particular de uma classe utilizaremos as *constantes* $a, a_0, a_1, \cdots$

Exemplo: Definindo as propriedades:

A representando a propriedade "ser morcego" para A(x) representar "x é um morcego",

B representando a propriedade "ser mamífero" para B(x) representar "x é mamífero",

as formalizações das frases:

a) Todos os morcegos são mamíferos;
b) Alguns morcegos são mamíferos;
c) Existem morcegos que não são mamíferos;
d) Não existem morcegos mamíferos,

são:

a) $\forall(x)(A(x) \rightarrow B(x))$;
b) $\exists(x)(A(x) \wedge B(x))$;
c) $\exists(x)(A(x) \wedge - B(x))$;
d) $\forall(x)(A(x) \rightarrow - B(x))$,

respectivamente.

Da mesma forma que no Cálculo Proposicional, podemos formalizar argumentos que agora envolvem expressões que representam quantidades. Considere o argumento:

Todo ator gosta de representar;
Raul é um ator;
Portanto, Raul gosta de representar.

Para formalizá-lo sejam:

A(x) representando “x é um ator”;

a representando “Raul”

e assim A(a) traduzirá “Raul é um ator”;

e seja ainda:

R(x) representando “x gosta de representar”

e assim R(a) significará “Raul gosta de representar”.

Percebe-se que agora a situação torna-se simples, pois o argumento dado acima, pode ser formalizado da seguinte maneira:

$$\frac{\begin{array}{c}\forall(x)(A(x) \rightarrow R(x)) \\ A(a)\end{array}}{R(a)}$$

Note que para obter a conclusão “Raul gosta de representar” a partir das premissas “Todo ator gosta de representar” e “Raul é um ator”, foi usada a regra de inferência *Modus Ponens*, fazendo a substituição da variável individual x pela constante individual a que significava “Raul”, nos predicados A e R, que tinham as duas a mesma variável. Isso é aceitável, pois a primeira expressão é uma afirmativa universal, ou seja, vale para todos os elementos do universo, e desde que “a” esteja neste conjunto, essa substituição pode ser realizada. Mais adiante formalizaremos este processo de substituir uma variável por uma constante.

Até agora, as propriedades envolveram uma única variável ou constante, e os predicados que as representam recebem então o nome de *predicados unários*. Algumas propriedades atuam sobre dois elementos ou mais, e assim devem ser representadas por predicados que se aplicam a várias variáveis ou constantes. Estes predicados recebem o nome *de predicados binários, ternários*, e assim sucessivamente.

Considere o argumento:

Todo professor de Daniel é professor de Leonardo;
Luciano é professor de Daniel;

Portanto, Luciano é professor de Leonardo.

A propriedade "ser professor" atua sobre duas variáveis ou constantes, pois alguém é professor de alguém. Então para formalizá-lo sejam:

$P(x_1,x_2)$ representando "x_1 é professor de x_2";

a_1 representando "Daniel";

a_2 representando "Leonardo";

a_3 representando "Luciano".

Assim $P(a_3,a_1)$ representará "Luciano é professor de Daniel" e $P(a_3,a_2)$ representará "Luciano é professor de Leonardo".

O argumento pode ser formalizado da seguinte maneira:

$$\forall(x_1)(P(x_1,a_1) \rightarrow P(x_1,a_1))$$
$$P(a_3,a_1)$$
$$\overline{}$$
$$P(a_3,a_2)$$

A regra de inferência usada foi *Modus Ponens*, e também foi feita a substituição da variável individual x_1 pela constante individual a_3 que significava "Luciano".

Observe que neste exemplo utilizamos um predicado binário.

Ao trabalharmos com predicados que se aplicam a várias variáveis ou constantes, a ordem das variáveis ou constantes nesse predicado não deve ser alterada, pois, por exemplo, se M representa a propriedade "se maior" então $M(x,x_0)$ representará "x é maior que x_0" e se mudarmos a ordem das variáveis x e x_0 teremos "x_0 é maior que x".

Da mesma forma que se P representa uma propriedade qualquer então P(x) formaliza "x possui a propriedade P" e - P(x) formalizará "x não possui a propriedade P", se $P(x_1,x_2)$ formaliza "x_1 está relacionado com x_2 pela propriedade P" então - $P(x_1,x_2)$ formalizará "x_1 não está relacionado com x_2 pela propriedade P".

Exemplo: Se $P(x_1,x_2)$ representa "x_1 é pai de x_2" então - $P(x_1,x_2)$ representará "x_1 não é pai de x_2".

Para estudarmos argumentos no Cálculo de Quantificadores nos falta ainda tratar das expressões que envolvem mais de um quantificador. Comecemos pelas que envolvem os dois quantificadores, $\forall$ e $\exists$. Como exemplo, considere a expressão:

$$\forall(x)(\exists(x_0)Q(x,x_0)),$$

a qual significa que, “para todo x, existe x_0, tal que x está relacionado com x_0 pela propriedade Q. Por exemplo, se Q representa a propriedade “ser maior”, $Q(x,x_0)$ representa “x é maior que x_0” e considerando que nosso universo é o conjunto dos números inteiros, a expressão dada nos diz que “para todo inteiro existe outro inteiro menor”, que como sabemos é verdadeira.

Por outro lado, considerando a expressão:

$$\exists(x)(\forall(x_0)Q(x,x_0)),$$

de acordo com as definições acima “existe um inteiro que é maior que qualquer outro inteiro”, que como sabemos é falsa.

Por isso afirmamos que o trato com este tipo de expressões deve ser feito com muito cuidado, observando-se não somente a ordem dos quantificadores, mas também o seu *escopo*, ou seja, a expressão sobre a qual ele atua, que é determinada pelo par de parênteses cuja abertura se dá imediatamente após ao quantificador, ou pela propriedade logo após este. Na expressão $\forall(x)(\exists(x_0)Q(x,x_0))$ o escopo do quantificador universal é $(\exists(x_0)Q(x,x_0))$ e o escopo do quantificador existencial é $Q(x,x_0)$.

No início deste capítulo vimos as principais expressões do Cálculo de Quantificadores: a universalização e a particularização e depois a afirmativa universal, a negativa universal, a afirmativa particular e a negativa particular, e também as respectivas negações. Para formalizar expressões mais gerais necessitamos compor essas expressões utilizando parênteses e conectivos lógicos, quando necessários. Todas essas expressões receberão o nome de *fórmulas bem formuladas predicadas – fbfp*, as quais trataremos simplesmente por *fórmulas*, e serão representadas por letras maiúsculas do alfabeto acompanhadas ou não por índices inferiores do conjunto dos números inteiros não negativos (Z_+). Devemos, porém, tomar bastante cuidado para não criar expressões que não tenham sentido no Cálculo de Quantificadores. Reforçamos que é muito importante saber identificar o escopo do quantificador, isto é, a parte da fórmula a qual o quantificador se aplica, o que, como vimos, geralmente é feito através de pares de parênteses ou de propriedade, logo após o quantificador.

Exemplo: Para a expressão "existem homens que amam todas as mulheres", definindo que A representa a propriedade "ser homem", B a propriedade "ser mulher" e C a propriedade "amar", temos que:

$A(x)$ representa "x é um homem";

$B(x)$ representa "x é uma mulher";

$C(x,x_0)$ representando "x ama x_0",

e assim a formalização da expressão dada é:

$$\exists(x)(A(x) \wedge \forall(x_0)(B(x_0) \rightarrow C(x,x_0))),$$

na qual o escopo do quantificador existencial é $(A(x) \wedge \forall(x_0)(B(x_0) \rightarrow C(x,x_0)))$ e o escopo do quantificador universal é $(B(x_0) \rightarrow C(x,x_0))$.

Da mesma forma que no Cálculo Proposicional, alguns pares de parênteses podem ser omitidos desde que isso não traga prejuízo à interpretação da fórmula.

Com as expressões que envolvem vários quantificadores, para facilitar a compreensão da formalização, pode ser interessante traduzi-las para uma *linguagem intermediária*, ou seja, para uma forma que não chega a ser uma sentença formalizada, mas também não é a forma como usualmente falamos ou escrevemos.

Exemplo: Para formalizar a expressão "todos os cachorros perseguem todos os gatos", primeiramente vamos traduzi-la para a linguagem intermediária "dada uma coisa qualquer, se for um cachorro, então, para qualquer outra coisa, se essa coisa for um gato, então o cachorro vai persegui-lo". Para formalizá-la sejam:

$A(x)$ representando "x é um cachorro";

$B(x)$ representando "x é um gato";

$C(x,x_0)$ representando "x persegue x_0".

Daí a sentença dada é:

$$\forall(x)(A(x) \rightarrow \forall(x_0)(B(x_0) \rightarrow C(x,x_0))).$$

Com as mesmas definições deste exemplo a expressão "alguns cachorros perseguem todos os gatos", que nos diz que "existe uma coisa que é um cachorro e, para qualquer outra coisa, se essa outra coisa é um gato, então o cachorro o persegue" é formalizada por:

$$\exists(x)(A(x) \wedge \forall(x_0)(B(x_0) \rightarrow C(x,x_0)\ C(x,x_0))),$$

e a expressão “alguns cachorros perseguem alguns gatos”, é formalizada por:

$$\exists(x)(A(x) \wedge \exists(x_0)(B(x_0) \wedge C(x,x_0))).$$

Ainda com as mesmas definições do último exemplo podemos formalizar a expressão “apenas cachorros perseguem gatos” por:

$$\forall(x_0)(\forall(x)(B(x_0) \wedge C(x,x_0) \rightarrow A(x))),$$

que intermediariamente pode ser compreendida como, “dadas duas coisas, se uma for um gato e a outra persegui-lo, então essa outra coisa é um cachorro”.

Uma variável x recebe o nome de *variável livre* quando ela não está associada em nenhum quantificador. Por exemplo, em $\forall(x)Q(x,x_0)$ x_0 é uma variável livre.

Observamos que uma fórmula com variáveis livres pode não ter um valor lógico em determinada interpretação. Por exemplo, se o universo é o conjunto dos números naturais, e com a interpretação na qual o predicado P(x) significa “x é par” e a representa o inteiro 10, a fórmula:

$$P(x_0) \wedge P(a)$$

não tem valor lógico, pois não sabemos a que elemento do universo x_0 se refere. Por outro lado, a fórmula:

$$P(x_0) \vee P(a)$$

é verdadeira com essa interpretação, embora não saibamos a que elemento do universo x_0 se refere.

Como já dissemos, no Cálculo de Quantificadores, para verificar se uma fórmula é verdadeira ou falsa dependemos da interpretação e do universo considerado. Assim, quando uma fórmula é verdadeira para uma determinada interpretação em um determinado universo, dizemos que essa fórmula é *válida para essa interpretação nesse universo*. Caso contrário, dizemos que a fórmula *não é válida para essa interpretação nesse universo*. Quando uma fórmula é sempre verdadeira, isto é, independentemente da interpretação e do universo, dizemos que a fórmula é simplesmente *válida*.

Exemplo: A fórmula:

$$\forall(x)(P(x) \vee Q(x)) \rightarrow (\forall(x)P(x) \vee \forall(x)Q(x))$$

não é válida quando o universo é o conjunto dos números naturais, com a interpretação de que P(x) significa que "x é par" e Q(x) significa que "x é ímpar", uma vez que o antecedente é verdadeiro, pois todo inteiro é par ou ímpar, mas o consequente é falso pois não é verdade que todo inteiro é par ou todo inteiro é ímpar.

Agora, se P(x) significa que "x é múltiplo de 2" e Q(x) significa que "x é múltiplo de 4" a fórmula do exemplo acima não é válida em $N_2 = \{2,4,6,8\cdots\}$ mas é válida em $N_4 = \{4,8,12\cdots\}$.

A fórmula:

$$\forall(x)(P(x) \wedge Q(x)) \rightarrow (\forall(x)P(x) \wedge \forall(x)Q(x))$$

como demonstraremos formalmente posteriormente é válida. No momento, podemos concordar com essa afirmação ao interpretá-la, pois sendo P e Q propriedades, se todo elemento possui as propriedades P e Q, então todo elemento possui a propriedade P e todo elemento possui a propriedade Q.

5.3 Lógica de predicados

Vimos nos exemplos anteriores, sem a devida formalização, que as Regras de Inferência estudadas no Cálculo Proposicional podem ser utilizadas também no Cálculo de Quantificadores, desde que alguns critérios sejam observados. Agora vamos formalizar esta aplicação.

Se $A_1, A_2, \cdots, A_n$ e B são fórmulas do Cálculo Proposicional, a validade do argumento $A_1, A_2, \cdots, A_n \vdash B$ pode ser verificada através de tabelas de verdade. O conceito sobre validade de argumentos é o mesmo no Cálculo de Quantificadores, no entanto, como já citamos, a veracidade de uma fórmula do Cálculo de Quantificadores dependerá do universo estabelecido e também da interpretação que realizamos.

Assim, a verificação da validade de um argumento no Cálculo de Quantificadores deve ser baseada apenas na estrutura interna do argumento, e não na veracidade ou falsidade das expressões em qualquer interpretação particular. Em outras palavras, o argumento deve ser válido em todas as interpretações possíveis. Como não existe nada equivalente a tabelas de verdade para provar a validade facilmente, vamos nos basear em um sistema lógico formal chamado *Lógica de Predicados*, o qual utiliza novamente as regras de inferência e as equivalências lógicas para construir uma sequência de demonstração que parta das hipóteses e chegue à conclusão, preservando os valores lógicos, de forma que, se em alguma interpretação todas as hipóteses forem verdadeiras, então a conclusão também será verdadeira com aquela interpretação.

Da mesma forma que no Cálculo Proposicional, se $A_1, A_2, \cdots, A_n$, B são fórmulas do Cálculo de Quantificadores de forma que podemos demonstrar a conclusão B a partir das premissas $A_1, A_2, \cdots, A_n$, dizemos que o conjunto de fórmulas $A_1, A_2, \cdots, A_n$, B é um argumento válido e denotamos por $A_1, A_2, \cdots, A_n \vdash B$. Para demonstrar este argumento devemos construir uma demonstração de B que assuma $A_1, A_2, \cdots, A_{n-1}$ e A_n como premissas, ou demonstrar B a partir de $(A_1 \wedge A_2 \wedge \cdots \wedge A_n)$, ou ainda, demonstrar que a fórmula $((A_1 \wedge A_2 \wedge \cdots \wedge A_n) \rightarrow B)$ é *válida*, isto é, é tautologia.

A abordagem geral para provar esses argumentos é retirar os quantificadores $\forall$ e $\exists$, manipular as fórmulas e depois recolocá-los. Para tanto existem quatro novas regras: uma para a retirada do quantificador universal, uma para a retirada do quantificador existencial, uma para a inserção do quantificador universal e uma para a inserção do quantificador existencial, as quais são apresentadas a seguir. Antes observamos que os exemplos que utilizaremos neste texto não visam privilegiar esta ou aquela forma de raciocínio, esta ou aquela área, na verdade são exemplos clássicos, já consagrados como eficientes na aprendizagem inicial no Cálculo de Quantificadores.

5.3.1 Particularização universal – PU

Essa regra diz que podemos deduzir $P(x)$, $P(x_0)$, $P(x_1)$, $P(a)$, $P(a_0)$, $P(a_1)$ etc. de $\forall(x)P(x)$, retirando, assim, um quantificador universal. A justificativa é que, se P é verdadeira para todos os elementos do universo, podemos nomear um tal elemento por um nome arbitrário de variável, como x, x_0, x_1 etc. ou podemos especificar uma constante particular no domínio a, a_0, a_1 etc., e P ainda é verdadeira para todas essas variáveis ou constantes.A particularização universal pode ser usada para provar um dos "silogismos" clássicos do filósofo e cientista grego Aristóteles, que viveu de 384 a 322 a.C. e foi o primeiro a desenvolver um sistema de lógica formal.

O argumento tem a forma:

Todos os humanos são mortais.
Sócrates é humano.
Portanto, Sócrates é mortal.

Usando a notação:

H(x) para denotar "x é humano";
a para denotar Sócrates;
M(x) para denotar "x é mortal";

a demonstração deste argumento é:

Demonstre: M(a)

(1) $\forall(x)(H(x) \rightarrow M(x))$	
(2) $H(a)$	
(3) $H(a) \rightarrow M(a)$	PU 1
(4) $M(a)$	MP 2, 3

No passo 3, um símbolo constante substituiu x em todo o escopo do quantificador universal, como permitido pela particularização universal.

Com outra notação, demonstramos o argumento:

$$\forall(x)(H(x) \rightarrow M(x)),\ H(a) \vdash M(a),$$

ou:

$$\forall(x)(H(x) \rightarrow M(x)) \wedge H(a) \vdash M(a).$$

A única restrição ao retirar $\forall(x)$ é que, se a variável x não deve figurar dentro do escopo de um quantificador que contenha outra variável x_0, a variável x não pode ser substituída por x_0, pois, por exemplo, uma hipótese da forma $\forall(x)\exists(x_0)P(x,x_0)$ poderia levar à $\exists(x_0)P(x_0,x_0)$, substituindo x por x_0 no escopo de um quantificador para x_0. Isso não é válido se o universo é o conjunto dos números inteiros e se $P(x,x_0)$ significa "$x < x_0$", então $\forall(x)\exists(x_0)P(x,x_0)$ é verdade, pois significa que para todo inteiro existe um inteiro maior, mas $\exists(x_0)P(x_0,x_0)$ é falso, pois nenhum inteiro tem a propriedade de ser maior do que si mesmo.

5.3.2 Particularização existencial E

Essa regra permite retirar um quantificador existencial. Ela diz que, a partir de $\exists(x)P(x)$, podemos deduzir $P(a)$, $P(a_0)$, $P(a_1)$ etc., desde que essas constantes sejam essencialmente novas. A justificativa é que, se P for verdadeira para algum elemento do universo, podemos dar um nome novo e específico a esse elemento, mas não podemos supor nada mais sobre ele, pois se assim fizermos podemos entrar em contradição com o grupo de elementos que possuem a propriedade P, delimitados em $\exists(x)P(x)$.

Exemplo: Demonstre: $Q(a_0)$

(1) $\forall(x)(P(x) \rightarrow Q(x))$	
(2) $\exists(x_0)P(x_0)$	
(3) $P(a_0)$	PE 2
(4) $P(a_0) \rightarrow Q(a_0)$	PU 1
(5) $Q(a_0)$	MP 3, 4

No passo 3, foi dado o nome a_0 ao elemento específico que tem a propriedade P. No passo 4, usou-se a PU para dizer que um condicional que é universalmente verdadeiro no domínio certamente é verdadeiro para esse a_0. A ordem dos passos 3 e 4 não pode ser trocada. Se PU tivesse sido utilizada primeiro em (1) para se nomear a constante a_0, não existiria nenhuma razão para supor que esse a_0 particular é o que tem a propriedade P como em (2).

Aqui demonstramos o argumento:

$$\forall(x)(P(x) \rightarrow Q(x)), \exists(x_0)P(x_0) \vdash Q(a_0),$$

que é o mesmo que:

$$\forall(x)(P(x) \rightarrow Q(x)) \wedge \exists(x_0)P(x_0) \vdash Q(a_0).$$

A restrição para o uso desta regra é que torna-se necessário que seja a primeira regra a utilizar as novas constantes. Assim, o efeito desta restrição é que primeiro devemos olhar todas as nossas hipóteses e se a PE for necessária, ela será feita em primeiro lugar.

5.3.3 Generalização universal – GU

A generalização universal permite que se insira um quantificador universal. Se soubermos que P(x) é verdadeiro e que x é um elemento absolutamente arbitrário, isto é, que x pode ser qualquer elemento no universo, então podemos concluir que $\forall(x)P(x)$. Mas se x representa algum elemento específico no domínio que tem a propriedade P, então não podemos generalizar que todo elemento no universo tem a propriedade P.

Exemplo: Demonstre: $\forall(x)Q(x)$

(1) $\forall(x)(P(x) \to Q(x))$	
(2) $\forall(x)P(x)$	
(3) $P(x) \to Q(x)$	PU 1
(4) $P(x)$	PU 2
(5) $Q(x)$	MP 3, 4
(6) $\forall(x)Q(x)$	GU 5

No exemplo acima demonstramos o argumento:

$$\forall(x)(P(x) \to Q(x)), \forall(x)P(x) \vdash \forall(x)Q(x),$$

ou:

$$\forall(x)(P(x) \to Q(x)) \wedge \forall(x)P(x) \vdash \forall(x)Q(x),$$

ou ainda que a fórmula:

$$\forall(x)(P(x) \to Q(x)) \wedge \forall(x)P(x) \to \forall(x)Q(x),$$

é válida.

A restrição de uso desta regra é que P(x) não pode ter sido deduzida de nenhuma hipótese na qual x é uma variável livre e nem pode ter sido deduzida através da regra PE de uma fórmula na qual x é uma variável livre.

5.3.4 Generalização existencial – GE

A última regra permite a inserção de um quantificador existencial. De P(x) ou P(a) podemos deduzir $\exists(x)P(x)$. Alguma coisa foi nomeada como tendo a propriedade P, logo, podemos dizer que existe alguma coisa que tem a propriedade P.

Observe o exemplo.

Exemplo: Demonstre: $\exists(x)P(x)$

(1) $\forall(x)P(x)$	
(2) $P(x)$	PU 1
(3) $\exists(x)P(x)$	GE 2

Aqui demonstramos o argumento:

$$\forall(x)P(x) \vdash \exists(x)P(x),$$

ou que a fórmula:

$$\forall(x)P(x) \to \exists(x)P(x),$$

é válida, ou seja, que de "todo x possui a propriedade P" podemos concluir que "algum x possui a propriedade P", ou que "se todo x possui a propriedade P então algum x possui a propriedade P", o que é bastante natural.

A restrição de uso aparece para predicados que atuam sobre várias variáveis. De P(x,a) não podemos deduzir $\exists(x)P(x,x)$, pois, por exemplo, no conjunto dos números naturais, se $P(x,x_0)$ representa "$x > x_0$" e a representa 10, P(x,a) representa os naturais maiores que 10 enquanto $\exists(x)P(x,x)$ afirma que existe natural maior que ele próprio.

Observe que, conforme já comentamos, é obviamente aceito que "se todo x possui as propriedades P e Q então todo x possui a propriedade P e todo x possui a propriedade Q", ou ainda que de "todo x possui as propriedades P e Q" podemos concluir que "todo x possui a propriedade P e todo x possui a propriedade Q". Isto é demonstrado no exemplo a seguir.

Exemplo: Use a lógica de predicados para provar o argumento:

$$\forall(x)(P(x) \wedge Q(x)) \vdash \forall(x)P(x) \wedge \forall(x)Q(x)$$

A nossa hipótese é:

(1) $\forall(x)(P(x) \wedge Q(x))$

e a demonstração é:

(2) $P(x) \wedge Q(x)$	PU 1
(3) $P(x)$	S 2
(4) $Q(x)$	S2
(5) $\forall(x)P(x)$	GU 3
(6) $\forall(x)Q(x)$	GU 4
(7) $\forall(x)P(x) \wedge \forall(x)Q(x)$	A 5, 6

Veja que com este exemplo demonstramos a validade da fórmula:

$$\forall(x)(P(x) \wedge Q(x)) \rightarrow \forall(x)P(x) \wedge \forall(x)Q(x),$$

já introduzida quando definimos a validade de fórmulas no Cálculo de Quantificadores.

Embora tenhamos adicionado apenas quatro regras de dedução novas, o conjunto de regras é *completo e correto*, isto é, podemos provar todos os argumentos válidos, e apenas esses, usando essas regras. A aplicação dessas regras, como no caso do

Cálculo Proposicional, é um tanto mecânica, já que existe apenas um número limitado de opções em cada passo.

Finalizando esta seção reafirmamos, como já fizemos no Cálculo Proposicional, que também no Cálculo de Quantificadores as regras de inferência podem ser aplicadas apenas quando as fórmulas envolvidas constituem exatamente a mesma forma especificada na regra e, é claro, quando nenhuma das restrições sobre as regra para exclusão ou inclusão de quantificadores for violada.

Além disso, na aplicação das regras para exclusão ou inclusão de quantificadores devemos tomar muito cuidado na observação do escopo de cada quantificador. Uma regra de particularização retira um quantificador da frente de uma fórmula inteira, que é o escopo desse quantificador. No entanto de:

$$\exists(x)P(x) \vee \exists(x)Q(x)$$

não podemos deduzir:

$$P(a) \vee Q(a)$$

utilizando PE, pois o escopo do primeiro quantificador existencial não se estende para o resto da fórmula.

Da mesma forma, de:

$$\forall(x)\exists(x_0)Q(x,x_0)$$

não podemos deduzir:

$$\forall(x)Q(x,a)$$

utilizando PE, pois o quantificador existencial não é o primeiro.

Por outro lado, as regras para inserir um quantificador colocam um quantificador na frente de uma fórmula que fica, então, inteiramente em seu escopo.

5.4 O método dedutivo no Cálculo de Quantificadores

O método dedutivo visto no capítulo Cálculo Proposicional ainda vale no Cálculo de Quantificadores. No teorema da dedução vimos que se Γ é um conjunto de fórmulas, A e B são fórmulas e $\Gamma, A \vdash B$, então $\Gamma \vdash (A \rightarrow B)$. Esse teorema nos permite demonstrar a validade do argumento $A_1, A_2, \cdots, A_n \vdash R \rightarrow S$ através do argumento$A_1, A_2, \cdots, A_n, R \vdash S$. Como consequência deste teorema, a um conjunto de premissas $A_1, A_2, \cdots, A_n$, podemos introduzir uma nova premissa, R, e daí, ao obtermos a conclusão S, demonstramos o argumento $A_1, A_2, \cdots, A_n, R \vdash S$, e pelo teorema da dedução demonstramos o argumento $A_1, A_2, \cdots, A_n \vdash R \rightarrow S$. A esta nova hipótese R introduzida daremos o nome de *hipótese temporária*.

Assim, o método dedutivo nos permitirá inserir uma hipótese temporária em uma demonstração. Se alguma fórmula R for inserida em uma sequência de demonstração e, finalmente, uma fórmula S for deduzida de R e de outras hipóteses, então a fórmula $R \rightarrow S$ pode ser deduzida, pelo teorema da dedução, das outras hipóteses e, portanto, pode ser considerada na sequência de demonstração. Isto será utilizado no próximo exemplo.

Exemplo: O argumento:

$$(P(x) \rightarrow \forall(x_0)Q(x,x_0)) \vdash \forall(x_0)(P(x) \rightarrow Q(x,x_0))$$

é válido. A demonstração é:

(1) $P(x) \rightarrow \forall(x_0)Q(x,x_0)$	
(2) $P(x)$	Hipótese temporária
(3) $\forall(x_0)Q(x,x_0)$	MP 1, 2
(4) $Q(x,x_0)$	PU 3
(5) $P(x) \rightarrow Q(x,x_0)$	Método dedutivo
(6) $\forall(x_0)(P(x) \rightarrow Q(x,x_0))$	GU 5

Veja que neste caso a hipótese temporária é exatamente o antecedente da condicional a ser demonstrada no argumento, permitindo a utilização do método dedutivo no passo (5).

No final do capítulo Cálculo Proposicional demonstramos que, utilizando uma contradição como premissa, podemos demonstrar qualquer fórmula que desejamos. Esse mesmo resultado vale no Cálculo de Predicados, e será utilizado no próximo exemplo e denotado por INC, sigla que vem da palavra "inconsistência".

Exemplo: Prove $-(\exists(x)P(x)) \leftrightarrow \forall(x)(-P(x))$

Sabemos que a fórmula $-(\exists(x)P(x)) \leftrightarrow \forall(x)(-P(x))$ é logicamente equivalente a fórmula:

$$-(((\exists(x)P(x)) \rightarrow \forall(x)(-P(x))) \wedge (\forall(x)(-P(x)) \rightarrow -(\exists(x)P(x))))$$

Assim, podemos demonstrar a validade da condicional em cada direção, isto é, podemos demonstrar a validade da fórmula $(- (\exists(x)P(x)) \rightarrow \forall(x)(- P(x)))$ e a validade da fórmula $(\forall(x)(- P(x)) \rightarrow - (\exists(x)P(x)))$.

Vamos então demonstrar a validade da fórmula:

$$(- (\exists(x)P(x)) \rightarrow \forall(x)(- P(x))),$$

ou seja, demonstrar a validade do argumento $- (\exists(x)P(x)) \vdash \forall(x)(- P(x))$:

(1) $- (\exists(x)P(x))$	
(2) $P(x)$	Hipótese temporária
(3) $\exists(x)P(x)$	GE, 2
(4) $P(x) \rightarrow \exists(x)P(x)$	Método dedutivo
(5) $- P(x)$	MT 1, 4
(6) $\forall(x)(- P(x))$	GU 5

Agora vamos demonstrar a validade da fórmula $(\forall(x)(- P(x)) \rightarrow - (\exists(x)P(x)))$, ou seja, demonstrar a validade do argumento $\forall(x)(- P(x)) \vdash - (\exists(x)P(x))$:

(1) $\forall(x)(- P(x))$	
(2) $\exists(x)P(x)$	Hipótese temporária
(3) $P(a)$	PE 2
(4) $- P(a)$	PU 1
(5) $P(a) \wedge - P(a)$	P 3, 4
(5) $- (\forall(x)(- P(x)))$	INC 5
(6) $\exists(x)P(x) \rightarrow - (\forall(x)(- P(x)))$	Método dedutivo
(7) $- (- (\forall(x)(- P(x))))$	DN 1
(8) $- (\exists(x)P(x))$	MT 6, 7

Veja que a hipótese temporária utilizada é exatamente o oposto do que queremos demonstrar.

A demonstração $- (\exists(x)P(x)) \leftrightarrow \forall(x)(- P(x))$ confirma que:

$$- (\exists(x)P(x)) \text{ é } \forall(x)(- P(x)),$$

conforme comentamos no início deste capítulo. Da mesma forma demonstra-se $- (\forall(x)P(x)) \leftrightarrow \exists(x)(- P(x))$,o que confirma que:

$$- (\forall(x)P(x)) \text{ é } \exists(x)(- P(x)),$$

também por nós comentado naquele momento.

Nessa mesma linha demonstra-se também que:

$$- (\forall(x)(- P(x))) \text{ é } \exists(x)P(x),$$

e que:

$$- (\exists(x)(- P(x))) \text{ é } \forall(x)P(x).$$

Desta forma, demonstramos o que intuitivamente já concluímos no início deste capítulo:

- $(\exists(x)P(x))$ é logicamente equivalente a $\forall(x)(-P(x))$;
- $(\forall(x)P(x))$ é logicamente equivalente a $\exists(x)(-P(x))$;
- $(\forall(x)(-P(x)))$ é logicamente equivalente a $\exists(x)P(x)$; e
- $(\exists(x)(-P(x)))$ é logicamente equivalente a $\forall(x)P(x)$.

A utilização de qualquer uma destas equivalências será de agora em diante denotada por NEG.

Exemplo: Prove a validade da fórmula $\forall(x)(P(x) \vee Q(x)) \rightarrow (\exists(x)P(x) \vee \forall(x)Q(x))$:

Essa fórmula nos diz que, se todo elemento no universo tem a propriedade P ou Q, então pelo menos um elemento tem a propriedade P, ou então todos os elementos tem a propriedade Q.

Vamos primeiro usar a equivalência notável, "Lei Condicional - LC" enunciada no capítulo Cálculo Proposicional para reescrever a conclusão, transformando a disjunção inclusiva em uma condicional, o que vai nos permitir utilizar o método dedutivo. Queremos, então, provar a validade da fórmula:

$$\forall(x)(P(x) \vee Q(x)) \rightarrow (-(\exists(x)P(x)) \rightarrow \forall(x)Q(x)),$$

que é o mesmo que provar a validade do argumento:

$$\forall(x)(P(x) \vee Q(x)) \vdash (-(\exists(x)P(x)) \rightarrow \forall(x)Q(x)).$$

Usando o método dedutivo podemos demonstrar a validade do argumento:

$$\forall(x)(P(x) \vee Q(x)), -(\exists(x)P(x)) \vdash \forall(x)Q(x),$$

cuja demonstração é:

(1) $\forall(x)(P(x) \vee Q(x))$	
(2) $-(\exists(x)P(x))$	
(3) $\forall(x)(-P(x))$	NEG 2
(4) $-P(x)$	PU 3
(5) $P(x) \vee Q(x)$	PU 1
(6) $(-(-P(x))) \vee Q(x)$	DN 5
(7) $(-P(x)) \rightarrow Q(x)$	LC 6
(8) $Q(x)$	MP 4, 7
(9) $\forall(x)Q(x)$	GU 8

Exemplo: Mostre que:

$$\exists(x)R(x) \wedge -(\exists(x)(R(x) \wedge S(x))) \vdash \exists(x)(-S(x))$$

é um argumento válido:

Este argumento nos diz que, se algo tem a propriedade R, mas nada tem ambas as propriedades R e S, então algo não tem a propriedade S.

A demonstração é:

(1) $\exists(x)R(x)$	
(2) $-(\exists(x)(R(x) \wedge S(x)))$	
(3) $\forall(x)(R(x) \rightarrow -S(x))$	Negação da afirmativa particular
(4) $R(a)$	PE 1
(5) $R(a) \rightarrow -S(a)$	PU 3
(6) $-S(a)$	MP 4, 5
(7) $\exists(x)(-S(x))$	GE 6

Este mesmo argumento pode ser demonstrado de outra forma:

(1) $\exists(x)R(x)$	
(2) $-((\exists x)(R(x) \wedge S(x)))$	
(3) $\forall(x)(-(R(x) \wedge S(x)))$	NEG 2
(4) $R(a)$	PE 1
(5) $-(R(a) \wedge S(a))$	PU 3
(6) $-R(a) \vee -S(a)$	DL 5
(7) $--R(a)$	DN 4
(8) $-S(a)$	TP 6, 7
(9) $\exists(x)(-S(x))$	GE 8

Este exemplo nos mostra que as demonstrações não são, em geral, únicas.

Destacamos que, sendo A e B propriedades quaisquer, as equivalências lógicas acima construídas:

$$-(\exists(x)P(x)) \text{ eq } \forall(x)(-P(x)),$$
$$-(\forall(x)P(x)) \text{ eq } \exists(x)(-P(x)),$$

nos apresentam outras formas da negações da afirmativa e negativa universais e da afirmativa e negativa existenciais:

$-(\exists(x)(A(x) \wedge B(x)))$ eq $\forall(x)(-(A(x) \wedge B(x)))$ eq $\forall(x)(-A(x) \vee -B(x))$;

$-\forall(x)(A(x) \rightarrow B(x))$ eq $\exists(x)(-(A(x) \rightarrow B(x)))$ eq $\exists(x)(A(x) \wedge -B(x))$;

$-(\exists(x)(A(x) \wedge -B(x)))$ eq $\forall(x)(-(A(x) \wedge -B(x)))$ eq $\forall(x)(-A(x) \vee B(x))$; e

$-(\forall(x)(A(x) \rightarrow -B(x)))$ eq $\exists(x)(-(A(x) \rightarrow -B(x)))$ eq $\exists(x)(A(x) \vee B(x))$.

5.5 Argumentos verbais

Para provar a validade de um argumento verbal, agora no Cálculo de Quantificadores, procedemos como no estudo da validade de um argumento verbal no Cálculo Proposicional. Escrevemos o argumento em forma simbólica e mostramos que conclusão pode ser deduzida das hipóteses.

Como já mencionamos, a Lógica Matemática não pode de fato preocupar-se com os argumentos verbais. No entanto, apresentamos o exemplo a seguir, pois ele nos mostra que não podemos tentar tratar situações do Cálculo de Quantificadores com o Cálculo Proposicional.

Exemplo: Mostre que o seguinte argumento é válido: “Todo microcomputador tem uma porta serial. Alguns microcomputadores têm uma porta paralela. Portanto, alguns microcomputadores têm uma porta serial e uma porta paralela.” usando a notação:

M(x) para representar “x é um microcomputador”;

S(x) para representar “x tem uma porta serial”;

P(x) para “x tem uma porta paralela”;

o argumento é:

$$\forall(x)(M(x) \to S(x)), \exists(x)(M(x) \wedge P(x)) \vdash \exists(x)(M(x) \wedge S(x) \wedge P(x)).$$

(1) $\forall(x)(M(x) \to S(x))$	
(2) $\exists(x)(M(x) \wedge P(x))$	
(3) $M(a) \wedge P(a)$	PE 2
(4) $M(a) \to S(a)$	PU 1
(5) $M(a)$	S 3
(6) $S(a)$	MP 4, 5
(7) $M(a) \wedge P(a) \wedge S(a)$	A 3, 6
(8) $M(a) \wedge S(a) \wedge P(a)$	CL 7
(9) $\exists(x)(M(x) \wedge S(x) \wedge P(x))$	GE 8

No Cálculo Proposicional, utilizando A para representar “todo microcomputador tem uma porta serial”, B para representar “alguns microcomputadores tem uma porta paralela” e C para representar “alguns microcomputadores tem uma porta serial e uma porta paralela” o nosso argumento é:

$$A, B \vdash C$$

o qual não é válido, pois a fórmula $((A \wedge B) \rightarrow C)$ não é tautologia. Isso acontece pois quando afirmamos que $M(x) \rightarrow S(x)$ vale para todo x, ou que $M(x) \wedge P(x)$ vale para alguns x, o Cálculo Proposicional não tem competência para tratar dessas quantidades.

5.6 Exercícios propostos

1) Usando os predicados E(x) para "x é um estudante", I(x) para "x é inteligente" e M(x) para "x gosta de matemática", escreva fórmulas que expressem as expressões a seguir, considerando o universo formado por todas as pessoas:

a) Todos os estudantes são inteligentes;
b) Alguns estudantes inteligentes gostam de matemática;
c) Todos que gostam de matemática são estudantes;
d) Apenas estudantes inteligentes gostam de matemática.

2) Encontre o valor lógico da fórmula:

$$\exists(x)(A(x) \wedge \forall(x_0)(B(x,x_0) \rightarrow C(x_0)))$$

no universo do conjunto dos números inteiros, com a interpretação de que A(x) significa que "$x > 0$", $B(x,x_0)$ significa que "$x > x_0$" e $C(x_0)$ é "$x_0 \leq 0$". Dê uma outra interpretação com o mesmo universo de modo que a proposição tenha valor lógico oposto.

3) Formalize os argumentos:

a)

Todo número par é múltiplo de 2;
10 é um número par;
Portanto, 10 é múltiplo de 2.

b)

Todo divisor de 10 é divisor de 20;
5 é divisor de 10;
Portanto, 5 é divisor de 20.

c)

Todo ator gosta de representar;
Augusto não gosta de representar;
Portanto, Augusto não é um ator.

4) Demonstre o argumento:

$$\forall(x)(P(x) \rightarrow R(x)) \wedge - R(x_0) \vdash - P(x_0).$$

5) Prove o argumento:

$$\forall(x)(P(x) \wedge Q(x)) \vdash \forall(x)(Q(x) \wedge P(x)).$$

6) Prove o argumento:

$$\forall(x_0)(P(x) \rightarrow Q(x,x_0)) \vdash (P(x) \rightarrow \forall(x_0) Q(x,x_0)).$$

7) Prove o argumento:

$$\forall(x)((B(x) \vee C(x)) \rightarrow A(x)) \vdash \forall(x)(B(x) \rightarrow A(x)).$$

6

Introdução à Teoria dos Conjuntos

Estudaremos neste capítulo a Teoria dos Conjuntos, e como o leitor perceberá, a fundamentação teórica já nos é familiar, pois, na verdade, conceitos estudados no Cálculo Proposicional serão revistos, agora com uma nova rotulação, e assim sugerimos que um paralelo entre o que agora estudaremos e o Cálculo Proposicional seja estabelecido.

Neste tópico não apresentaremos a maioria das demonstrações de resultados e propriedades, visto que são perfeitamente aceitáveis ou justificados quando traçamos, como já sugerimos, um paralelo entre o que aqui estudaremos e o Cálculo Proposicional. Para os estudantes interessados nessas demonstrações, apresentamos algumas e propomos outras como exercícios no final do capítulo.

O conceito de conjunto aparece em todos os ramos da matemática, e intuitivamente, um *conjunto* é qualquer lista ou coleção bem definida de objetos e será indicado por letras maiúsculas do alfabeto. Os objetos componentes do conjunto são denominados *elementos* ou *membros* e serão indicados por letras minúsculas do alfabeto.

A afirmação "p é um elemento de A" ou, equivalentemente, "p pertence a A", é indicada por:

$$p \in A$$

A negação de $p \in A$ é indicada por:

$$p \notin A$$

Existem, essencialmente, dois modos de se especificar um conjunto particular. Um modo é, quando possível, listar todos os seus elementos. Por exemplo:

$$A = \{a,e,i,o,u\}$$

indica o conjunto A, cujos elementos são as letras a, e, i, o, e u. Note-se que os elementos são separados por vírgulas e inclusos em chaves, e a quantidades de elementos não pode ser muito grande. O segundo modo é enunciar as propriedades que caracterizam os elementos do conjunto ou a lógica de formação desses elementos. Por exemplo:

$$B = \{x|x \text{ é um interiro e } x > 0\},$$

que se lê "B é o conjunto dos x, tais que x é um inteiro e x é maior que zero", indica o conjunto B cujos elementos são os números inteiros positivos. Neste modo, uma letra minúscula do alfabeto, geralmente x, é usada para indicar um elemento típico do conjunto, e a barra vertical significa "tal que" e após ela citamos a(s) propriedade(s) que o elemento típico satisfaz. O conjunto $A = \{a, e, i, o, u\}$ também pode ser escrito como:

$$A = \{x|x \text{ é uma letra do alfabeto e } x \text{ é uma vogal}\},$$

e o conjunto $B = \{x|x \text{ é um interiro e } x > 0\}$ também pode ser escrito como:

$$A = \{1,2,3,4,\cdots\},$$

quando apresentamos o primeiro elemento e em seguida outros que permitem identificar a lei de formação de seus elementos. Neste caso, a partir do segundo elemento este será igual ao anterior acrescido de uma unidade.

Exemplo: Considere o conjunto:

$$E = \{x|x^2 - 3x + 2 = 0\},$$

formado pelos números que são soluções da equação:

$$x^2 - 3x + 2 = 0,$$

ou seja, o conjunto solução da equação dada. Como as soluções da equação são 1 e 2, também poderíamos escrever:

$$E = \{1,2\}.$$

Definição: Dois conjuntos A e B são *iguais* e escrevemos A = B se eles são formados pelos mesmos elementos, isto é, se e somente se cada elemento de A pertence a B e cada elemento de B pertence a A. Formalizando:

$$A = B \leftrightarrow \forall(x)((x \in A \rightarrow x \in B) \wedge (x \in B \rightarrow x \in A)).$$

A negação de A = B é indicada por $A \neq B$, e significa que algum elemento de A não é elemento de B ou algum elemento de B não é elemento de A. Formalizando:

$$A \neq B \leftrightarrow \exists(x)((x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A)).$$

Exemplo: Sejam $E = \{x|x^2 - 3x + 2 = 0\}$, $F = \{2,1\}$ e $G = \left\{1,2,2,1,\frac{6}{3}\right\}$.

Então, E = F = G.

Observemos que um conjunto não depende da maneira pela qual seus elementos são mostrados. Um conjunto permanece o mesmo se seus elementos são repetidos ou reordenados.

Definição: Um conjunto é *finito* se consiste de exatamente n elementos diferentes, em que n é algum inteiro positivo, caso contrário, é *infinito*.

Exemplos:

1) Seja M o conjunto dos dias da semana, isto é:

M = {domingo, segunda, terça, quarta, quinta, sexta, sábado}, então M é finito.

2) Seja Y = {2,4,6,8}. Y é infinito.

Definição: Um conjunto A é um *subconjunto* de um conjunto B e indica-se:

$$A \subseteq B \text{ ou } B \supseteq A,$$

se e somente se cada elemento de A também pertence a B, isto é, se $x \in A$, então $x \in B$. Formalizando:

$$A \subseteq B \leftrightarrow \forall(x)(x \in A \rightarrow x \in B).$$

Podemos também dizer que A está *contido* em B, ou ainda que B *contém* A. A notação $A \subset B$ é utilizada quando cada elemento de

A também pertence a B e B possui algum elemento que não está em A. Em outras palavras $A \subseteq B$ significa que $A \subset B$ ou $A = B$. A negação de $A \subseteq B$ ou de $A \subset B$ é indicada por $A \not\subset B$ e afirma que existe pelo menos um $x \in A$ tal que $x \notin B$. Formalizando:

$$A \not\subset B \leftrightarrow \exists(x)(x \in A \wedge x \notin B).$$

Exemplo: Consideremos os conjuntos:

$$A = \{1,3,5,7,\cdots\},$$

$$B = \{5,10,15,20,\cdots\},$$

e

$$C = \{x|x \text{ é primo e } x > 2\} = \{3,5,7,11,\cdots\}.$$

Observe que $C \subset A$ pois todo número primo maior do que dois é ímpar. Por outro lado, $B \not\subset A$ pois, por exemplo, $10 \in B$, mas $10 \notin A$.

Também é conveniente introduzir o conceito de conjunto vazio, isto é, um conjunto que não contém nenhum elemento, e que é denotado por $\{\ \}$ ou $\varnothing$. O conjunto vazio é subconjunto de todos os outros conjuntos e dele próprio, ou seja, se A é um conjunto qualquer então $\varnothing \subseteq A$.

Exemplo: Seja $A = \{x|x^2 = 4 \text{ e } x \text{ é ímpar}\}$. Então A é vazio, isto é, $A = \{\ \} = \varnothing$.

Observe que de acordo com a última definição todo conjunto A é subconjunto dele mesmo, isto é, $A \subseteq A$. Também decorre dessa definição que dados dois conjuntos A e B, $A \subseteq B$ e $B \subseteq A$ se e somente se $A = B$, uma nova definição para a igualdade de dois conjuntos A e B.

Se $A \subseteq B$ e $A \neq B$, o que denotamos por $A \subset B$, e $A \neq \varnothing$, dizemos que A é um *subconjunto próprio* de B, ou que B *contém propriamente* A. O conjunto vazio e o próprio B são ditos *subconjuntos impróprios* de B.

Teorema: Sejam A, B, e C conjuntos. Se $A \subseteq B$ e $B \subseteq C$ então $A \subseteq C$.

Demonstração: Seja $x \in A$. Como $A \subseteq B$ cada elemento de A também pertence a B. Assim $x \in B$. Como $B \subseteq C$ cada elemento de B também pertence a C. E assim $x \in C$, o que mostra que $A \subseteq C$ como queríamos.

Em qualquer estudo da Teoria dos Conjuntos, todos os conjuntos em questão são considerados como subconjuntos de um conjunto fixo. Denominamos este conjunto de conjunto universo e o indicaremos por U.

Exemplos:

1) Na geometria plana, o conjunto universo é o conjunto formado por todos os pontos do plano.

2) Nos estudos sobre a população humana, o conjunto universo é formado por todas as pessoas do mundo.

Frequentemente, os elementos de um conjunto também são conjuntos. Por exemplo, cada reta de um conjunto de retas é um conjunto de pontos. Assim, temos as seguintes definições.

Definição: Chama-se *classe* ou *coleção* um conjunto de conjuntos, ou seja, um conjunto no qual seus elementos também são conjuntos. S*ubclasse* ou *subcoleção* são definidos de forma análoga a definição de subconjunto.

Exemplo: Os elementos da classe $\{\{2,3\}, \{2\}, \{5,6\}\}$ são os conjuntos $\{2,3\}$, $\{2\}$ e $\{5,6\}$.

Definição: Dado um conjunto A, chama-se *conjunto das partes de A*, que é indicado por P(A) ou 2^A, a classe de todos os subconjuntos de A.

Exemplo: Se $A = \{a\}$ então $2^A = \{A, \varnothing\}$. Se $B = \{a,b\}$ então $2^B = \{A,\varnothing,\{a\},\{b\}\}$. Se $C = \{a,b,c\}$, então $2^C = \{A,\varnothing,\{a\},\{b\},\{c\},\{a,b\},\{a,c\},\{b,c\}\}$.

Observe que se A é finito, com n elementos, então P(A) possui 2^n elementos.

6.1 Operações com conjuntos

Definição: A *reunião* ou *união* de dois conjuntos A e B, indicada por $A \cup B$, é o conjunto de todos os elementos que pertencem a A ou a B:

$$A \cup B = \{x|x \in A \text{ ou } x \in B\}.$$

Definição: A *interseção* de dois conjuntos A e B, indicada por $A \cap B$, é o conjunto de todos os elementos que pertencem a A e a B:

$$A \cap B = \{x|x \in A \text{ e } x \in B\}.$$

Se $A \cap B = \varnothing$ isto é, se A e B não tem nenhum elemento comum, então dizemos que A e B são *disjuntos*. Agora, se $A \cup B = \varnothing$ então $A = \varnothing$ e $B = \varnothing$.

Definição: O *complementar relativo* de um conjunto B com respeito a um conjunto A ou, simplesmente, a diferença de A e B, indicada por $A \backslash B$ ou $A - B$ ou ainda $C_A B$, é o conjunto dos elementos que pertencem a A, mas não pertencem a B:

$$A \backslash B = \{x | x \in A \text{ e } x \notin B\}.$$

Veja que nesta definição não exigimos que $B \subseteq A$. Alguns autores deixam a notação $C_A B$ exclusiva para quando temos $B \subseteq A$, o que não será adotado neste texto.

Definição: O *complementar absoluto* ou, simplesmente, complementar de um conjunto A, indicado por A^C ouC_A é o conjunto dos elementos que não pertencem a A:

$$A^C = \{x | x \in U \text{ e } x \notin A\}.$$

Observe que o complementar absoluto de um conjunto A é a diferença do conjunto universo e A.

Exemplo: Sejam:

$$A = \{1,2,3,4\}$$

e

$$B = \{3,4,5,6,7\},$$

em que $U = \{1,2,3,4,5,\cdots\} = \mathbb{Z}^*_+$. Então:

$$A \cup B = \{1,2,3,4,5,6,7\}$$
$$A \cap B = \{3,4\}$$
$$A \backslash B = \{1,2\}$$
$$B \backslash A = \{5,6,7\}$$
$$A^C = \{5,6,7,8,\cdots\}$$

Teorema: Sejam A, B, e C conjuntos quaisquer. Valem as seguintes propriedades, conhecidas como as leis da álgebra dos conjuntos:

1) Leis Idempotentes:

a) $A \cup A = A$;

b) $A \cap A = A$.

2) Leis Associativas:

a) $(A \cup B) \cup C = A \cup (B \cup C)$;

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

3) Leis Comutativas:
   a) $A \cup B = B \cup A$;
   b) $A \cap B = B \cap A$.
4) Leis Distributivas:
   a) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$;
   b) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.
5) Leis de Identidade:
   a) $A \cup \varnothing = A$;
   b) $A \cap \varnothing = \varnothing$;
   c) $A \cup U = U$;
   d) $A \cap U = A$.
6) Leis de Complementação:
   a) $A \cup A^C = U$;
   b) $A \cap A^C = \varnothing$;
   c) $(A^C)^C = A$;
   d) $U^C = \varnothing$;
   e) $\varnothing^C = U$.
7) Leis de De Morgan:
   a) $(A \cup B)^C = A^C \cap B^C$;
   b) $(A \cap B)^C = A^C \cup B^C$.

Vamos demonstrar a primeira das leis de De Morgan. Seja então $x \in (A \cup B)^C$. Logo $x \notin A \cup B$ e assim $x \notin A$ e $x \notin B$. Logo $x \in A^C$ e $x \in B^C$ ou $x \in A^C \cap B^C$, e, portanto, $(A \cup B)^C \subseteq A^C \cap B^C$. Analogamente se mostra que $A^C \cap B^C \subseteq (A \cap B)^C$, concluindo que $(A \cap B)^C = A^C \cap B^C$.

Fica claro a semelhança entre as leis acima e as equivalências lógicas denominadas Equivalências Notáveis, apresentadas no capítulo Cálculo Proposicional. Veja, como exemplo, a segunda lei comutativa:

$A \cap B = \{x | x \in A \text{ e } x \in B\} = \{x | x \in B \text{ e } x \in A\} = B \cap A$.

Usamos, aqui, o fato de que se a variável proposicional p representa "$x \in A$" e a variável proposicional q representa "$x \in B$", temos que $(p \wedge q)$ é logicamente equivalente a $(q \wedge p)$ pela Equivalência Notável Lei Comutativa. Por isso não nos preocuparemos com as demonstrações das demais leis.

Teorema: Sejam A e B conjuntos quaisquer. Cada uma das seguintes condições é equivalente a $A \subseteq B$:

a) $A \cap B = A$;
b) $A \cup B = B$;
c) $B^C \subseteq A^C$;
d) $A \cap B^C = \varnothing$;
e) $B \cup A^C = U$.

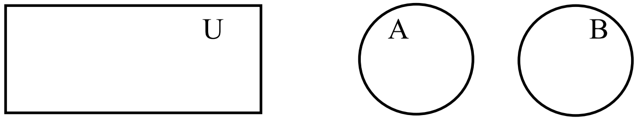
A validade deste teorema fica bem compreendida quanto utilizamos os diagramas de Euler-Venn, que veremos a seguir, e a demonstração, bastante simples, é deixada a cargo do leitor.

6.2 Diagramas de Euler-Venn

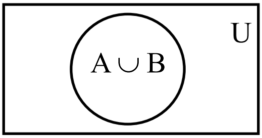
Entre 1770 e 1772, Leonard Euler utilizou diagramas em "Cartas a uma princesa da Alemanha" para exemplificar os quatro tipos de expressões do Cálculo de Quantificadores, nosso objeto de estudo no próximo capítulo:

Todo X é Y;
Algum X é Y;
Nenhum X é Y;
Algum X não é Y.

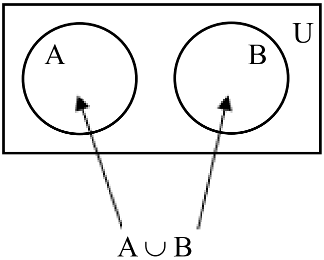
Em 1880, John Venn propôs nova forma de diagramas circulares, dando uma interpretação mais elucidativa. Nestes diagramas, sendo U o conjunto universo e A e B dois conjuntos em U, estes são representados por:



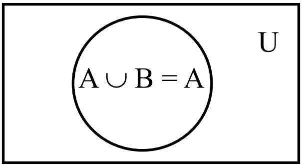
Com estas representações, podemos compreender as operações e propriedades acima estudadas, como por exemplo, o diagrama de $A \cup B = \{x | x \in A \text{ ou } x \in B\}$ quando $A = B$ é:



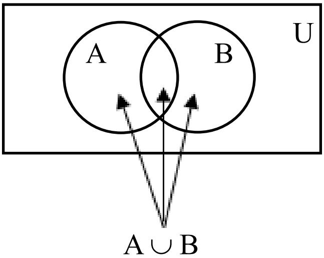
Agora, se $A \neq B$ temos os casos:
i) $A \cap B = \varnothing$, isto é, A e B são disjuntos:



ii) $A \cap B \neq \varnothing$, com $B \subseteq A$:

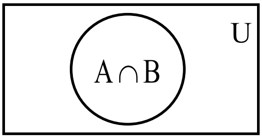


iii) $A \cap B \neq \varnothing$, e nenhum deles está contido no outro:



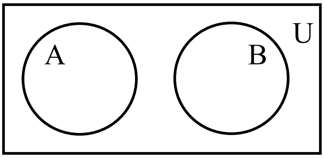
Outros casos particulares, como por exemplo, quanto um deles é o conjunto vazio ou quando um deles é o conjunto universo, entre outros, serão deixados a cargo do leitor.

Veja agora que o diagrama de $A \cap B = \{x | x \in A \text{ e } x \in B\}$, com $A = B$ é:



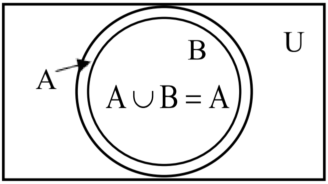
Agora quando $A \neq B$ temos os casos:

i) A e B disjuntos:

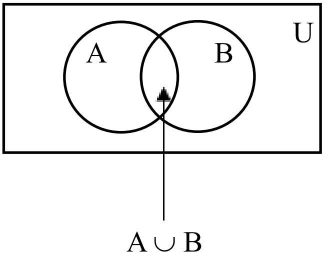


$A \cap B = \varnothing$

ii) $A \cap B \neq \varnothing$, com $B \subset A$:



iii) $A \cap B \neq \varnothing$, e nenhum deles está contido no outro:



Outros casos particulares, como por exemplo, quanto um deles é o conjunto vazio ou quando um deles é o conjunto universo, entre outros, serão deixados a cargo do leitor.

6.3 Exercícios propostos

1) Seja A = $\{x|3 \cdot x = 6\}$ É verdade que A = 2?

2) Verifique quais dos seguintes conjuntos:

$$\{t,r,s\},\ \{s,t,r,s\},\ \{t,s,t,r\} \text{ e } \{s,r,s,t\}$$

são iguais.

3) Verifique quais dos seguintes conjuntos são finitos:

a) O conjunto dos meses do ano

b) $\{1,2,3,\cdots,99,100\}$

c) O conjunto das pessoas que vivem na Terra

d) $\{1,2,3,4,5,\cdots\}$

e) $\{x|x \text{ é um número par}\}$.

4) Determine quais dos seguintes conjuntos, $\emptyset$, $\{0\}$ e $\{\emptyset\}$ são iguais.

5) Determine se algum destes conjuntos é o conjunto vazio:

$$X = \{x|x^2 = 9 \text{ e } 2 \cdot x = 4\},$$
$$Y = \{x|x \neq x\},$$
$$Z = \{x|x + 8 = 8\}.$$

6) Verifique se cada afirmação é verdadeira ou falsa:

a) Todo subconjunto de um conjunto finito é finito.

b) Todo subconjunto de um conjunto infinito é infinito.

7) Mostre que A = $\{2,3,4,5\}$ não é um subconjunto de B = $\{x|x \text{ é par}\}$.

8) Determine o conjunto das partes de A e o conjunto das partes de B, quando A= $\{1,2,3,4\}$ e B = $\{1, \{2,3\},4\}$.

9) Sejam: $A = \{1,2,3,4,5,6,7,8,9\}$, $B = \{2,4,6,8\}$, $C = \{1,3,5,7,9\}$, $D = \{3,4,5\}$ e $E = \{3,5\}$.

Verifique entre os conjuntos acima, qual(is) pode(m) ser igual(is) a X se:

a) X e B são disjuntos;

b) $X \subseteq D$, mas $X \not\subset B$;

c) $X \subseteq A$, mas $X \not\subset C$.

10) Sejam:

$V = \{d\}$, $W = \{c,d\}$, $X = \{a,b,c\}$, $Y = \{a,b\}$ e $Z = \{a,b,d\}$

Determine se cada afirmação é verdadeira ou falsa:

a) $Y \subseteq X$

b) $W \neq Z$

c) $Z \supseteq V$

d) $V \subseteq X$

e) $X = W$

f) $W \subseteq Y$.

11) Sejam $U = \{a,b,c,d,e,f,g\}$, $A = \{a,b,c,d,e\}$, $B = \{a,c,e,g\}$ e $C = \{b,e,f,g\}$. Determine:

a) $A \cup C$

b) $B \cap A$

c) $C \backslash B$

d) $B^C \cup C$

e) $C^C \cap A$

f) $(A \backslash C)^C$

g) $(A \backslash B^C)^C$

h) $(A \cap A^C)^C$.

12) A fórmula $A \backslash B = A \cap B^C$ define a operação de diferença em função de operações de interseção e complementação. Encontre:

a) Uma fórmula que defina a reunião de dois conjuntos quaisquer A e B, em função das operações de interseção e complementação

b) Uma fórmula que defina a interseção de dois conjuntos quaisquer A e B, em função das operações de reunião e complementação.

13) Sejam:

$U = \{1,2,3,4,5,6,7,8,9\}$, $A = \{1,2,3,4\}$, $B = \{2,4,6,8\}$ e $C = \{3,4,5,6\}$.

Encontre:

a) A^C

b) $A \cap C$

c) $(A \cap C)^C$

d) $A \cup B$

e) $B \backslash C$.

14) Demonstre que $B \backslash A = B \cap A^C$.

15) Demonstre que $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

16) Demonstre que $(A \backslash B) \cap B = \varnothing$.

17) Demonstre que $(A \cup B)^C = A^C \cap B^C$.

18) Demonstre que: $A \cap B \subseteq A \subseteq A \cup B$.

19) Demonstre que se $A \cap B = \varnothing$ então $A \subseteq B^C$.

20) Demonstre que $A^C \backslash B^C = B \backslash A$.

21) Demonstre que $A \subset B$ implica $A \cup (B \backslash A) = B$.

22)

a) Demonstre $A \cap (B \backslash C) = (A \cap B) \backslash (A \cap C)$

b) Dar um exemplo para mostrar que:

$$A \cup (B \backslash C) \neq (A \cup B) \backslash (A \cup C).$$

23) Represente o conjunto A\B através de diagramas de Venn nos seguintes casos:

a) A e B disjuntos

b) $B \subset A$

c) $A \cap B \neq \emptyset$, mas nenhum deles está contido no outro.

7

Álgebra Superior e a álgebra Booleana

Nosso objetivo neste capítulo é conhecer a álgebra Booleana, em particular a álgebra dos computadores, mas, antes temos um longo caminho a percorrer. Estudaremos estruturas algébricas, quando conceitos por nós já utilizados ou simplesmente conhecidos serão definidos formalmente como este estudo exige, como por exemplo, o conceito de operação em um conjunto, por nós já conhecido e praticado desde nossa infância quando conhecemos as operações com números.

Depois, no Cálculo Proposicional conhecemos e praticamos as operações com função de verdade, e neste capítulo veremos uma definição geral de operação, para a qual todas as operações que conhecemos são casos particulares, ou se preferir, exemplos. Este estudo nos mostrará que a álgebra Booleana é um exemplo de uma estrutura algébrica, e a álgebra dos computadores é uma álgebra Booleana particular.

Como neste capítulo muitas demonstrações serão realizadas, preliminarmente vamos realizar uma breve apresentação das técnicas de demonstração. Na verdade, essas técnicas já foram utilizadas ao longo desta obra, e agora vamos apenas denominá-las e praticar alguns poucos exemplos, pois na verdade a prática acontecerá em muitos outros momentos da sua vida acadêmica ou profissional.

As principais técnicas de demonstração podem ser divididas em dois grupos:

i) demonstrações diretas, e

ii) demonstrações indiretas.

Antes de apresentarmos cada um desses grupos, lembramos que uma afirmação pode não exigir demonstração, ou seja, ser uma verdade absoluta, isto é, uma tautologia. Neste momento não são estas que nos interessam, pois, agora nosso objeto de estudo é a afirmação que exige uma demonstração. A grande maioria delas tem a forma $A \rightarrow B$, outras a forma $A \leftrightarrow B$, a qual como sabemos é logicamente equivalente a $(A \rightarrow B) \wedge (B \rightarrow A)$.

7.1 Demonstrações diretas

Estas demonstrações são as que realizamos justificando cada passo com as regras de inferência, com as equivalências lógicas ou com as regras para a retirada ou inclusão de quantificadores. Embora já tenhamos visto muitas, vamos recordá-la.

Toda demonstração direta deve começar com as premissas A_1, A_2, $\cdots$, A_n, a partir das quais são aplicadas regras de inferência, equivalências lógicas ou regras para a retirada ou inclusão de quantificadores, até chegar à conclusão B, sendo que cada conclusão obtida em cada passo constitui mais uma premissa a ser considerada para o próximo passo, e cada passo deve ser justificado com a apresentação do que foi aplicado e quais premissas foram envolvidas. É obvio que tautologias podem ser inseridas em qualquer demonstração, em qualquer momento. Quando obtemos B, demonstramos que de $A_1 \wedge A_2 \wedge \cdots \wedge A_n$ podemos concluir B, ou que $A_1 \wedge A_2 \wedge \cdots \wedge A_n$ implica logicamente B, ou ainda que as fórmulas A_1, A_2, $\cdots$, A_n implicam logicamente a fórmula B.

Como na condicional, se o antecedente é falso a condicional é verdadeira, e assim nada temos a demonstrar, este tipo de demonstração só faz sentido quando todas as premissas forem verdadeiras, pelo menos em suposição.

Exemplo: Se eu trabalhar e poupar então comprarei um barco. Se comprar um barco, então conhecerei o mundo. Como eu trabalho, portanto, se não conheço o mundo então não poupei.

Demonstração: Conforme vimos no tópico Argumentos Verbais, sendo:

p: trabalhar,

q : poupar,

r : comprar um barco, e

p_0: conhecer o mundo,

o enunciado anterior podemos escrever na forma:

$$((p \wedge q) \rightarrow r) \wedge (r \rightarrow p_0) \wedge p \vdash (- p_0 \rightarrow - q)$$

o qual é o mesmo que:

$$((p \wedge q) \rightarrow r) \wedge (r \rightarrow p_0) \wedge p \wedge - p_0 \vdash - q$$

pelo Teorema da Dedução.

(1) $(p \wedge q) \rightarrow r$	
(2) $r \rightarrow p_0$	
(3) p	
(4) $- p_0$	
(5) $(p \wedge q) \rightarrow p_0$	HS 1, 2
(6) $- p_0 \rightarrow - (p \wedge q)$	LC 5
(7) $- (p \wedge q)$	MP 4, 6
(8) $- p \vee - q$	DL 7
(9) $- - p$	DN 3
(10) $- q$	TP 8, 9

Exemplo: Demonstrar que, se $x^2 + 2 \cdot x \geq 3$ e $x = 2 \cdot a - 1$, então, $a^2 \geq 1$.

Demonstração: Sejam:

$p : x^2 + 2 \cdot x \geq 3$,

$q : x = 2 \cdot a - 1$, e

$r : a^2 \geq 1$.

Devemos demonstrar r a partir da premissa $p \wedge q$.

(1) $p \wedge q$: $x^2 + 2 \cdot x \geq 3 \wedge x = 2 \cdot a - 1$
(2) p: $x^2 + 2 \cdot x \geq 3$ S1
(3) q: $x = 2 \cdot a - 1$ S1
(4) $(2 \cdot a - 1)^2 + 2 \cdot (2 \cdot a - 1) \geq 3$ Substituição
(5) $4 \cdot a^2 \geq 4$
(6) q: $a^2 \geq 1$

A demonstração direta pode ainda ser realizada através de um contraexemplo. Na verdade, esse tipo de demonstração é utilizada para demonstrar que determinada afirmação não é válida e tem por base que "não é verdade que todo elemento x possui a propriedade p" é logicamente equivalente a "existe algum elemento x que não possui a propriedade p", conforme vimos no tópico Noções sobre Cálculo de Quantificadores.

Exemplo: Demonstrar que para todo natural n, tem-se $n + 1 = 5$.

Demonstração: Suspeitamos que o argumento é falso. Assim nos basta encontrar um número natural n tal que $n + 1 = 5$ não seja verdade.

Considere $n = 10$ e assim $10 + 1 = 11$.

Logo, existe um número natural n tal que $n + 1 = 5$ é falso.

Portanto, não é verdade que, para todo natural n, temos $n + 1 = 5$.

7.2 Demonstrações indiretas

A demonstração indireta é uma técnica na qual uma afirmação é confirmada a partir da verificação da falsidade obtida ao supor o oposto.

Entre os métodos de demonstrações indiretas, estudaremos os seguintes:

a) por contraposição;
b) por casos;
c) por redução ao absurdo; e
d) por árvore de refutação.

7.2.1 Demonstração indireta por contraposição

Consiste na verdade na aplicação da lei condicional:

$$A \rightarrow B \text{ eq } - B \rightarrow - A,$$

ou seja, em vez de demonstrarmos $A \rightarrow B$ demonstramos $- B \rightarrow - A$, e nesta demonstração utilizamos a demonstração direta.

7.2.2 Demonstração indireta por casos

Este método é na verdade o método da dedução por nós já estudado, segundo o qual se de $A_1, A_2, \cdots, A_n, A$ podemos concluir B então de $A_1, A_2, \cdots, A_n$, podemos concluir $A \rightarrow B$, e assim se temos as premissas $A_1, A_2, \cdots, A_n$, para demonstrar a conclusão $A \rightarrow B$ podemos utilizar a fórmula A também como premissa para então de $A_1, A_2, \cdots, A_n, A$ concluirmos B. Este método já foi por nós demonstrado no teorema da dedução, e também várias vezes utilizado, quando vimos que usando uma premissa adicional A podemos facilitar ou simplificar a demonstração. Assim, apenas justificaremos o seu nome agora apresentado: demonstração indireta por casos.

Se de $A_1, A_2, \cdots, A_n, A$ ou de $A_1 \wedge A_2 \wedge \cdots \wedge A_n \wedge A$, podemos concluir B, ou seja, se B é consequência lógica de $A_1, A_2, \cdots, A_n, A$, então B é consequência lógica de A_1, B é consequência lógica de $A_2, \cdots$, B é consequência lógica de A_n, e B é consequência lógica de A, ou seja, em todos os casos, as implicações, valem, ou ainda, todas as premissas implicam logicamente a conclusão. O outro lado também é verdadeiro, isto é, se cada uma das premissas $A_1, A_2, \cdots, A_n, A$ implicam logicamente a conclusão B então de $A_1, A_2, \cdots, A_n, A$ ou de $A_1 \wedge A_2 \wedge \cdots \wedge A_n \wedge A$ podemos concluir B.

7.2.3 Demonstração indireta por redução ao absurdo

A demonstração por absurdo mostra a falsidade de uma suposição derivando dela um absurdo flagrante. Em geral, a utilização deste método para provar que uma conclusão B é verdadeira consiste na suposição da negação de B, o que nos conduzirá a um absurdo, seja mostrando uma afirmação - A sendo que A já foi mostrada anteriormente ou mesmo mostrando que B é verdadeira.

Como exemplo demonstraremos que existe um número infinito de números primos, um dos teoremas mais importantes da Teoria dos Números.

Vamos supor então que não existem infinitos números primos.

Por definição, sabemos que os números primos são os números naturais maiores do que 1 e que somente podem ser decompostos como o produto de dois fatores: ele mesmo e a unidade. São eles:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, \cdots$$

Sabemos também que todo número natural maior que 1 pode ser escrito como o produto de fatores primos.

Pela nossa suposição existe um último primo U, ou seja, os números primos são:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, \cdots, U.$$

Considere então o número $V = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot (U + 1)$.

V é maior do que U e assim V não pode ser primo, o que implica que pelo menos um dos primos 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, …, U divide V, o que não é verdade. Logo V é primo e U não é o maior dos números primos, e assim é falso que não existem infinitos números primos.

7.3 Algoritmo da divisão – múltiplos ou divisores

Usualmente os números nos são apresentados na base decimal, mas a álgebra dos computadores está fundamentada na base binária e a ferramenta que nos permite a conversão de bases, como veremos, é o algoritmo da divisão. Antes, porém, este algoritmo se fará presente na demonstração de importantes resultados que caracterizam uma importante relação da Álgebra Superior, a relação de equivalência módulo m. Nessa relação, como veremos, o conceito de múltiplo ou de divisor são essenciais e como este está intimamente relacionado com o algoritmo da divisão os apresentaremos previamente. Este algoritmo se deve a Euclides, e por isso também é conhecido como *algoritmo de Euclides*:

Dados dois números inteiros n e d, com $d > 0$, existem dois números inteiros q e r tais que $n = q \cdot d + r$, com $0 \leq r < d$. Além disso, os números q e r são únicos, para cada par de números n e d dados.

Demonstração:

A demonstração deste algoritmo é realizada em duas partes. Na primeira mostramos a existência dos inteiros q e r e na segunda mostramos que eles são únicos.

(i) Existência:

Suponha inicialmente que n é um número natural.

Vamos usar o princípio da indução, fazendo a indução sobre n.

Para $n = 1$, tem-se $q = 1$ e $r = 0$ no caso $d = 1$, pois $1 = 1 \cdot 1 + 0$. No caso $d > 1$, tem-se $q = 0$ e $r = 1$, uma vez que $1 = 0 \cdot d + 1$.

Suponhamos o algoritmo válido para $n = k$, isto é, $k = q \cdot d + r$, com $0 \leq r < d$.

Desse modo, $k + 1 = q \cdot d + r + 1$. Como $0 \leq r \leq d - 1$, analisemos os casos $0 \leq r \leq d - 2$ e $r = d - 1$ separadamente.

Para $r = d - 1$, temos $r + 1 = d$, e assim $k + 1 = q \cdot d + d = d \cdot (q + 1)$. Logo, $k + 1$ dividido por d tem $q + 1$ como quociente e resto zero.

Agora, para $0 \leq r \leq d - 2$, temos $1 \leq r + 1 \leq d - 1$. Assim, $k + 1 = q \cdot d + r + 1$, em que $1 \leq r + 1 \leq d - 1$. Portanto, o algoritmo também é válido para $n = k + 1$.

Portanto, pelo princípio da indução, o algoritmo é válido para todo número natural n.

Para $n = 0$, tem-se zero como quociente e resto, pois $0 = 0 \cdot d + 0$.

Se $n < 0$, de $n = q \cdot d + r$, com $0 \leq r < d$, segue que se $r = 0$, temos:

$$-n = -q \cdot d + 0,$$

e caso contrário:

$$-n = -q \cdot d - r = -q \cdot d - d + d - r = (-q - 1) \cdot d + (d - r),$$

e como $0 \leq r < d$, então, $0 < d - r < d$.

Desse modo, o algoritmo é válido para todo inteiro negativo.

Portanto, o algoritmo é válido para todo inteiro n.

(ii) Unicidade:

Agora vamos mostrar que os números inteiros q e r são únicos, para cada par de números inteiros n, d dado. Vamos supor que existam dois inteiros u e v, tais que $n = q \cdot d + r$ e $n = u \cdot d + v$, com $0 \leq r < d$ e $0 \leq v < d$. Vamos supor que $u < q$. Logo, $u + 1 \leq q$, pois u e q são inteiros. Podemos concluir que:

$$r = n - q \cdot d \leq n - (u + 1) \cdot d = n - u \cdot d - d = v - d < 0,$$

o que é uma contradição, pois $r \geq 0$.

O mesmo raciocínio pode ser usado para o caso em que $u > q$, para obter uma contradição.

Logo só resta $u = q$. Portanto, temos $n = q \cdot d + r$ e $n = q \cdot d + v$, o que implica $r = v$. E assim a unicidade está provada, concluindo a nossa demonstração.

De acordo com o algoritmo de Euclides, dados dois números inteiros n e d, com $d > 0$, existem dois números inteiros q e r, tais que $n = q \cdot d + r$, com $0 \leq r < d$. O conceito de *múltiplo* ou *divisor* é um caso especial desse algoritmo: quando $r = 0$ temos $n = q \cdot d$ quando dizemos que n é múltiplo de d ou que d divide n, o que simbolizamos por $d \mid n$.

7.4 Relações, aplicações e operações

Definição: Dados dois conjuntos não vazios A e B, define-se o *produto cartesiano* de A e B como sendo o conjunto $AxB = \{(x,y) \mid x \in A \text{ e } y \in B\}$. Além disso, se $B = \{\ \}$, então, $Ax\{\ \} = \{\ \} = \{\ \}xA$, onde $\{\ \}$ representa o conjunto vazio.

Exemplo: Sendo $A = \{2,3\}$ e $B = \{3,4,5\}$, temos:

$$AxB = \{(2,3),(2,4),(2,5),(3,3),(3,4),(3,5)\}.$$

Definição: Sendo A e B dois conjuntos, chama-se *relação* de A em B ou entre A e B qualquer subconjunto de AxB.

Exemplo: Sendo $A = \{2,3\}$ e $B = \{3,4,5\}$, os conjuntos $R = \{(2,3),(2,4),(2,5)\}$, $S = \{(3,3)\}$, $T = \{(2,3),(3,5)\}$, $\{\ \}$ e AxB são exemplos de relações de A em B.

Sendo R uma relação de um conjunto A em um conjunto B, isto é, $R \subseteq AxB$, o domínio de R é o conjunto:

$$D(R) = \{x \in A \mid \exists (y),\ y \in B \text{ com } (x,y) \in R\},$$

e a imagem de R é o conjunto:

$$Im(R) = \{y \in B \mid \exists (x),\ x \in A \text{ com } (x,y) \in R\}.$$

Notação: Se $(x,y) \in R$, onde R é uma relação de um conjunto A em um conjunto B escrevemos xRy e dizemos que x está associado a y pela relação R ou x se relaciona com y através da relação R.

Definição: Sendo A e B dois conjuntos e R uma relação de A em B, a *relação inversa* de R é o conjunto:

$$R^{-1} = \{(y,x) \in BxA \ |(x,y) \in R\}.$$

Observe que R^{-1} é uma relação de B em A.

Exemplos:

1) Sendo:

$A = \{1,2,3,5\}$,

$B = \{3,4,6,9\}$

e

$R = \{(1,4),(3,6),(3,9),(5,3)\}$,

temos que:

$D(R) = \{1,3,5\}$,

$Im(R) = \{3,4,6,9\}$,

$R^{-1} = \{(4,1),(6,3),(9,3),(3,5)\}$,

$D(R^{-1}) = \{3,4,6,9\} = Im(R)$

e

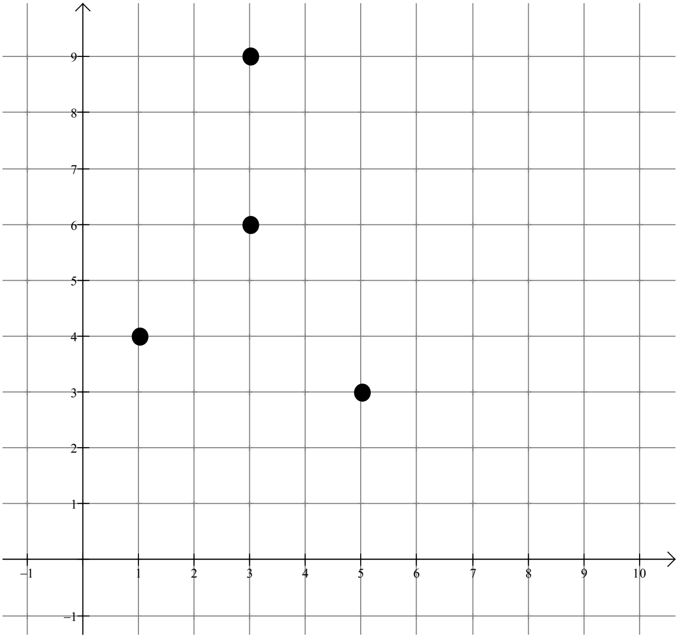
$Im(R^{-1}) = \{1,3,5\} = D(R)$.

2) Sendo A e B o conjunto dos números naturais, isto é, A = B = N, considere a relação R dada por:

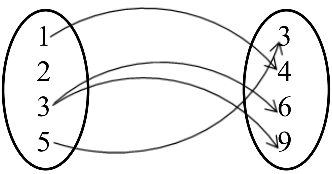
$$R = \{(x,y) \in NxN|x < y\}.$$

R é uma relação, pois $R \subset NxN$ e $D(R) = N$, $Im(R) = N - \{1\}$, $R^{-1} = \{(x,y) \in NxN|x > y\}$, $D(R^{-1}) = N - \{1\}$ e $Im(R^{-1}) = N$.

Quando A e B são subconjuntos finitos do conjunto dos números reais, podemos representar graficamente uma relação qualquer de A em B usando o plano cartesiano. Voltando ao exemplo 1 anterior, temos a seguinte representação gráfica da relação R:



Quando A e B são conjuntos finitos podemos representar graficamente uma relação qualquer de A em B usando diagrama de flechas. A relação R do exemplo anterior pode ser assim representada por um diagrama de flechas:



Definição: Dado um conjunto não vazio A, uma *relação em A* é uma relação de A em A.

Definição: Dado um conjunto não vazio A, uma relação R em A diz-se uma *relação de equivalência* em A se satisfaz as seguintes condições:

i) $\forall(x)(x \in A \rightarrow xRx)$, ou seja, para todo $x \in A$, $(x,x) \in R$.

ii) $\forall(x,y)(x,y \in A \wedge xRy \rightarrow yRx)$, ou seja, para quaisquer $x,y \in A$, se $(x,y) \in R$, então, $(y,x) \in R$.

iii) $\forall(x,y,z)(x,y,z \in A \wedge xRy \wedge yRz \rightarrow xRz)$, ou seja, para quaisquer $x,y,z \in A$, se $(x,y) \in R$ e $(y,z) \in R$ então $(x,z) \in R$.

Quando R satisfaz i) dizemos que R é reflexiva. Quando R satisfaz ii) dizemos que R é simétrica. Quando R satisfaz iii) dizemos que R é transitiva.

Exemplos:

1) Seja R a relação em Q definida por $(x,y) \in R$ se e se somente se $x - y \in Z$. R é uma relação de equivalência, pois para quaisquer $x,y,z \in Q$, temos:

i) $(x,x) \in R$, pois $x - x = 0 \in Z$. Logo R é reflexiva.

ii) Se $(x,y) \in R$, então, $x - y \in Z$, e, assim, $y - x = -(x - y) \in Z$, ou seja, $(y,x) \in R$. Logo R é simétrica.

iii) Se $(x,y) \in R$ então, $x - y \in Z$. Se $(y,z) \in R$ então, $y - z \in Z$. Somando-se, obtemos $x - y + y - z = a + b$, com $a = x - y$ e $b = y - z$. Como $a \in Z$ e $b \in Z$ temos que $a + b \in Z$, ou seja, $x - z \in Z$, e assim $(x,z) \in R$. Logo R é transitiva.

2) Seja A um conjunto não vazio. Seja R uma relação em A definida por:

$$R = \{(x,y) \in AxA | x = y\},$$

a qual também pode ser descrita por:

$$xRy \leftrightarrow x = y.$$

R é uma relação de equivalência, e a demonstração ficará a cargo do leitor.

3) Seja A o conjunto dos números reais e definamos a relação S em A por:

$$S = \{(x,y) \in AxA | x^2 = y^2\},$$

a qual também pode ser descrita por:

$$xSy \leftrightarrow x^2 = y^2.$$

S é uma relação de equivalência em A , e a demonstração ficará a cargo do leitor.

4) Em N, isto é, sendo A o conjunto dos números naturais, considere a relação:

$$R = \{(a,b) \in NxN | a \leq b\}.$$

R não é uma relação de equivalência em N, uma vez que R não é simétrica em N, pois existem a,b $\in$ N, com $a \leq b$ e $b > a$, o que pode ser comprovado escolhendo, por exemplo, a = 1 e b = 2.

5) Seja A = {1,2,3}. Considere as relações em A:

R = {(1,1),(2,2),(3,3),(1,3),(3,2)};

S = {(1,2),(2,3),(1,3)};

T = {(1,2),(2,1)}; e

R = {(1,1),(1,2),(2,2),(2,3),(3,3),(1,3),(3,2)}.

R é reflexiva, R não é simétrica e R não é transitiva.

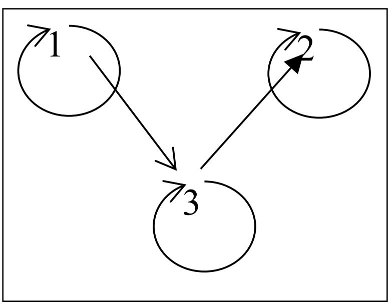
S não é reflexiva, S não é simétrica e S é transitiva.

T não é reflexiva, T é simétrica e T não é transitiva.

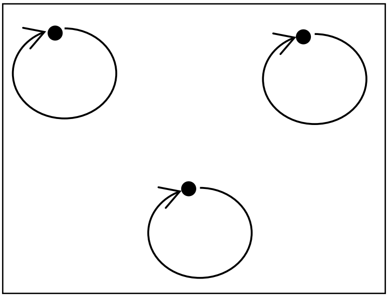
U é reflexiva, U não é simétrica e U é transitiva.

Notação: É usual denotar uma relação de equivalência R em um conjunto A por ~, isto é, usualmente escreve-se x ~ y, em vez de xRy.

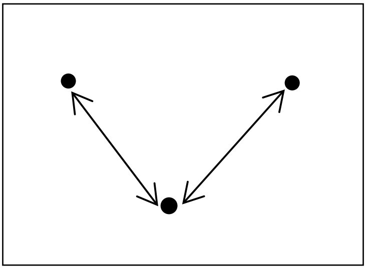
Quando A é um conjunto finito o diagrama de flechas que representa uma relação qualquer em A pode ser simplificado. A relação R do exemplo 5 proposto pode ser assim representada:



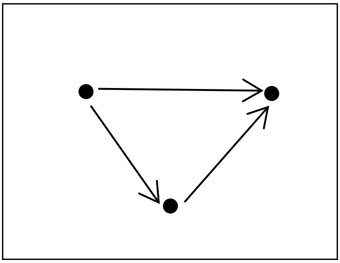
Observe que nesta representação a propriedade reflexiva é válida se e somente se em cada elemento do diagrama houver um laço:



a propriedade simétrica será válida se e somente se toda flecha tiver duas pontas:



e a propriedade transitiva será válida se para todo par de flechas consecutivas existir uma flecha cuja origem é a origem a primeira e o final é o final da segunda.



Definição: Seja $A \neq \{\ \}$ e seja R uma relação de equivalência em A. Dado $a \in A$, chama-se *classe de equivalência* de a, módulo R, ou segundo R, o conjunto $\bar{a} = \{x \in A | xRa\}$.

O conjunto das classes de equivalência de uma relação de equivalência R em um conjunto A, não vazio, chama-se *conjunto quociente* de A pela relação R e é denotado por A\R.

Proposição: Seja ~ uma relação de equivalência em um conjunto não vazio A e sejam $a,b,c \in A$. As seguintes afirmações são equivalentes:

$a \sim b$;

$a \in \bar{b}$;

$b \in \bar{a}$;

$\bar{a} = \bar{b}$.

Demonstração:

Veja que $a \sim b \Rightarrow \bar{a} \in \bar{b}$.

Agora $a \sim b \Rightarrow b \sim a$, pois ~ é comutativa, e $b \sim a \Rightarrow b \in \bar{a}$.

Também $b \in \bar{a} \Rightarrow b \sim a$ e $b \sim a \Rightarrow a \sim b$, pois ~ é comutativa.

Logo $1 \Rightarrow 2 \Rightarrow 3 \Rightarrow 1$ e assim 1, 2 e 3 são equivalentes.

Precisamos ainda mostrar agora que 4 é equivalente a 1, 2 ou 3. Vamos mostrar que $4 \Leftrightarrow 1$.

Tomemos por hipótese $\bar{a} = \bar{b}$.

Agora se $\bar{a} = \bar{b}$ então $a \in \bar{b}$, pois $a \in \bar{a}$, e assim $a \sim b$, concluindo que $4 \Rightarrow 1$.

Agora tomemos por hipótese $a \sim b$.

Sabemos que para qualquer $x \in A$, $x \in \bar{a}$, se e somente se $x \sim a$.

Agora, se $x \sim a$ e $a \sim b$, então, $x \sim b$, pois ~ é transitiva, e assim $x \in \bar{b}$.

Logo se $x \in \bar{a}$, então, $x \in \bar{b}$, ou seja, $\bar{a} \subseteq \bar{b}$.

Analogamente se verifica que $\bar{b} \subseteq \bar{a}$. Logo $\bar{a} = \bar{b}$, e assim concluímos que $1 \Rightarrow 4$, encerrando nossa demonstração.

Veja que desta última proposição conclui-se que duas classes de equivalência são iguais ou são disjuntas.

Exemplos:

1) Seja A = {1,2,3,4} e consideremos a relação em A:

~ = {(1,1),(2,2),(3,3),(4,4),(1,3),(2,3),(3,1),(3,2),(1,2),(2,1)}.

~ é uma relação de equivalência em A e as suas classes de equivalência são:

$\bar{1} = \{1,2,3\}$,

$\bar{1} = \bar{2} = \bar{3}$ pois como 2 ~ 1, então pela proposição $\bar{2} = \bar{1}$ e como 3 ~ 1, então pela proposição $\bar{3} = \bar{1}$,

$\bar{4} = \{4\}$.

Assim, o conjunto quociente de A pela relação ~ é $A\backslash\sim = \{\bar{1}, \bar{4}\} = \{\{1,2,3\}, \{4\}\}$.

2) Seja A = R. Seja S uma relação em A definida por:

$$S = \{(x,y) \in AxA | x = y\}.$$

Para qualquer x ∈ R, temos que $\bar{x} = \{x\}$ e $R\backslash S = \{\{x\} | x \in R\}$.

Definição: Seja m > 1 um número inteiro. Dados a,b ∈ Z, dizemos que a é *côngruo* a b módulo m se e somente se m | (a – b), isto é, m divide a diferença entre a e b, o que denotamos por a ≡ b (mod m) ou $a \underset{m}{\equiv} b$.

Observe que dizer que m | (a – b) é o mesmo que dizer que a – b é múltiplo de m, ou seja, m | (a – b) se e somente se a – b = k · m para algum k ∈ Z.

Agora vamos justificar a escolha m > 1, na definição de côngruos acima. Veja que se:

i) se m = 0, então para quaisquer a,b ∈ Z, $a \underset{0}{\equiv} b$ se e somente se a – b = k · 0 para algum k ∈ Z, ou seja, se e somente se a = b.

ii) se m = 1, então para quaisquer a,b ∈ Z, $a \underset{1}{\equiv} b$ se e somente se a – b = k · 1 para algum k ∈ Z, isto é, 1|(a – b). Logo, para quaisquer a,b ∈ Z temos $a \underset{1}{\equiv} b$.

iii) se m < 0, então para quaisquer a,b ∈ Z, $a \underset{m}{\equiv} b$, se e somente se a – b = k · m para algum k ∈ Z. Ou seja, se e somente se b – a = – k · m para algum k ∈ Z, ou seja, $b \underset{m}{\equiv} a$, que é o mesmo que $a \underset{m}{\equiv} b$, sem nada acrescentar, desde que esta relação seja de equivalência, como de fato é, o que demonstraremos a seguir, após as duas seguintes proposições, que nos fornecem outras caracterizações da congruência módulo m.

Proposição: Seja $m > 1$ um número inteiro. Dados $a,b \in Z$, a é côngruo a b módulo m se e somente se a e b deixam o mesmo resto na divisão por m.

Demonstração:

Suponhamos primeiramente que a é côngruo a b módulo m, ou seja que $m \mid (a - b)$. Seja r_1 o resto da divisão de a por m e seja r_2 o resto da divisão de b por m, ou seja:

$$a = k_1 \cdot m + r_1, \text{ com } k_1 \in Z \text{ e } 0 \leq r_1 < m, \text{ e}$$
$$b = k_2 \cdot m + r_2, \text{ com } k_2 \in Z \text{ e } 0 \leq r_2 < m.$$

Subtraindo a segunda igualdade acima da primeira obtemos:

$$a - b = (k_1 - k_2) \cdot m + r_1 - r_2.$$

Como, por suposição, $m \mid (a - b)$, temos que $r_1 - r_2 = 0$, ou seja, $r_1 = r_2$.

Suponhamos agora que a e b deixam o mesmo resto na divisão por m e seja r este resto. Logo:

$$a = k_1 \cdot m + r, \text{ com } k_1 \in Z \text{ e } 0 \leq r < m, \text{ e}$$
$$b = k_2 \cdot m + r, \text{ com } k_2 \in Z \text{ e } 0 \leq r < m.$$

Subtraindo a segunda igualdade acima da primeira obtemos:

$$a - b = (k_1 - k_2) \cdot m,$$

o que mostra que $m \mid (a - b)$, ou seja, que a é côngruo a b módulo m.

Proposição: Seja $m > 1$ um número inteiro. Se a deixa resto r na divisão por m então a é côngruo a r módulo m.

Demonstração:

Se a deixa resto r na divisão por m então $a = k \cdot m + r$, com $k \in z$ e $0 \leq r < m$. Como $r = 0 \cdot m + r$, pela proposição acima temos que a é côngruo a r módulo m.

Observe que a segunda das duas proposições acima é um caso especial da primeira, e assim vale também que se a é côngruo ao seu resto r na divisão por m módulo m então a deixa resto r na divisão por m, o que é óbvio.

Exemplos:

1) $21 \equiv 1 (\text{mod } 5)$ pois $21 - 1 = 20$ é divisíve por 5.

2) $14 \equiv 2 (\text{mod } 12)$ pois $14 - 2 = 12$ é divisível por 12.

Vamos agora demonstrar que a congruência módulo m é uma relação de equivalência. Veja que para todo $a,b,m \in Z$, $m > 1$, temos que:

i) $a \equiv a(\text{mod } m)$ pois $a - a = 0$ é divisível por m.

ii) $a \equiv b(\text{mod } m)$, então $m \mid (a - b)$ ou $a - b = k \cdot m$ para algum $k \in Z$. Daí $b - a = -(a - b) = -k \cdot m$ e assim $m \mid (b - a)$ e portanto $b \equiv a(\text{mod } m)$.

iii) Se $a \equiv b(\text{mod } m)$ e $b \equiv c(\text{mod } m)$ então $a - b = k_1 \cdot m$ para algum $k_1 \in Z$ e $b - c = k_2 \cdot m$ para algum $k_2 \in Z$. Daí:

$$a - c = a - b + b - c = (k_1 + k_2) \cdot m,$$

ou seja, $m|(a - c)$, ou seja, $a \equiv c(\text{mod } m)$.

Logo, a congruência módulo m em Z é reflexiva, simétrica e transitiva, ou seja, é uma relação de equivalência, a qual recebe o nome de relação de congruência. O conjunto quociente dessa relação, o qual indicamos por Z_m, é $\{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{m-1}\}$. Vamos à demonstração.

i) Dado $a \in Z$, temos $a = k \cdot m + r$, com $k \in Z$ e $0 \leq r < m$. Logo $a - r = km$, e assim $a \equiv r(\text{mod } m)$, ou ainda $\overline{a} = \overline{r}$. Como $r \in \{0,1,2,3, \cdots, m - 1\}$ temos que $\bar{a} \in \{0,1,2,3, \cdots,m - 1\}$.

ii) Suponhamos agora que existam duas classes iguais em $\{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{m-1}\}$, isto é, $\overline{u} = \overline{v}$ com $0 \leq u < v < m$. Neste caso temos $u \equiv v$ (mod m) e assim $m \mid (u - v)$ como também $m \mid (v - u)$. Como $u < v$ temos $v - u > 0$ e assim $0 < v - u < m$, o que é um absurdo.

Logo o número de elementos de Z_m é exatamente m.

Exemplo: Seja $m = 5$ e consideremos a relação de equivalência $a \equiv b(\text{mod } m)$. Temos que:

$$\overline{0} = \left\{a \in Z \middle| a \underset{5}{\equiv} 0\right\} = \left\{a \in Z \middle| 5 \mid (a - 0)\right\} = \left\{5 \cdot k \middle| k \in Z\right\} = \{\cdots,-5,0,5,10,\cdots\}$$

$$\overline{1} = \left\{a \in Z \middle| a \underset{5}{\equiv} 1\right\} = \left\{a \in Z \middle| 5 \mid (a - 1)\right\} = \left\{5 \cdot k + 1 \middle| k \in Z\right\} = \{\cdots,-5,1,6,11,\cdots\}$$

$$\overline{2} = \left\{a \in Z \middle| a \underset{5}{\equiv} 2\right\} = \left\{a \in Z \middle| 5 \mid (a - 2)\right\} = \left\{5 \cdot k + 2 \middle| k \in Z\right\} = \{\cdots,-3,2,7,12,\cdots\}$$

$$\overline{3} = \left\{a \in Z \middle| a \underset{5}{\equiv} 3\right\} = \left\{a \in Z \middle| 5 \mid (a - 3)\right\} = \left\{5 \cdot k + 3 \middle| k \in Z\right\} = \{\cdots,-2,3,8,13,\cdots\}$$

$$\overline{4} = \left\{a \in Z \middle| a \underset{5}{\equiv} 4\right\} = \left\{a \in Z \middle| 5 \mid (a - 4)\right\} = \left\{5 \cdot k + 4 \middle| k \in Z\right\} = \{\cdots,-1,4,9,14,\cdots\}$$

$\overline{5} = \overline{0}$;

$\overline{6} = \overline{1}, \cdots$

Veja ainda que $\overline{-1} = \overline{4}$, $\overline{-2} = \overline{3}$, $\overline{-3} = \overline{2}$, $\overline{-4} = \overline{1}$, $\overline{-5} = \overline{0}$, $\cdots$ e assim $Z_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$.

Definição: Dado um conjunto não vazio A, uma relação R em A diz-se uma *relação de ordem parcial* em A se satisfaz as seguintes condições:

i) $\forall(x)(x \in A \to xRx)$, ou seja, para todo $x \in A$, $(x,x) \in R$.

ii) $\forall(x,y)(x,y \in A \wedge xRy \wedge yRx \to x = y)$, ou seja, para quaisquer $x,y \in A$, se $(x,y) \in R$ e $(y,x) \in R$ então $x = y$.

iii) $\forall(x,y,z)(x,y,z \in A \wedge xRy \wedge yRz \to xRz)$, ou seja, para quaisquer $x,y,z \in A$, se $(x,y) \in R$ e $(y,z) \in R$ então $(x,z) \in R$.

A condição ii recebe o nome de propriedade antissimétrica. Veja então que se R é uma relação de ordem parcial em A então R é reflexivantissimétrica e transitiva.

Quando R é uma relação de ordem parcial em A, é comum denotar $(a,b) \in R$ por $a \leq b(R)$, que se lê “a precede b na relação R”. Quando $(a,b) \in R$ e $a \neq b$ denotaremos por $a < b(R)$ e lemos “a precede estritamente b na relação R”.

Definição: Um *conjunto parcialmente ordenado* é um conjunto sobre o qual se definiu alguma relação de ordem parcial.

Definição: Seja R uma relação de ordem parcial sobre A. Os elementos $a,b \in A$ se dizem *comparáveis* se $a \leq b(R)$ ou $b \leq a(R)$.

Definição: Se dois elementos quaisquer de A forem comparáveis mediante uma relação R, então R será chamada de *relação de ordem total* sobre A e o conjunto A, neste caso, é chamado de *conjunto totalmente ordenado*.

Exemplos:

1) A relação $R = \{(1,1),(2,2),(3,3),(1,2),(2,3),(1,3)\}$ é uma relação de ordem total sobre $A = \{1,2,3\}$.

2) A relação $R = \{(a,a),(b,b),(c,c),(a,b),(b,c),(a,c)\}$ é uma relação de ordem total sobre $A = \{a,b,c\}$.

3) A relação S sobre o conjunto dos números reais dada por $S = \{(x,y) \in RxR | x \leq y\}$ é uma relação de ordem total.

4) A relação de divisibilidade sobre o conjunto dos números naturais, $xRy \leftrightarrow x \mid y$ é uma relação de ordem parcial.

5) A igualdade é uma relação de ordem parcial em um conjunto não vazio qualquer A.

6) As relações xRy $\leftrightarrow$ x < y e xRy $\leftrightarrow$ x > y não são relações de ordem, pois não são reflexivas.

Definição: Seja f uma relação de A em B. Dizemos que f é uma *aplicação* de A em B se e somente se:

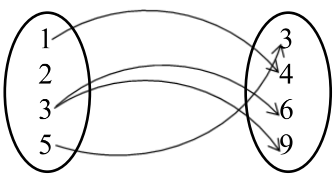
i) D(f) = A;

ii) Dado a $\in$ D(f), é único o elemento b $\in$ B, tal que (a,b) $\in$ f.

Se f for uma aplicação de A em B, escrevemos b = f(a) para indicar que b é a imagem de a pela aplicação f, ou seja, que (a,b) $\in$ f e f : A $\rightarrow$ B é a maneira simbólica de dizermos que f é uma aplicação de A em B. Será usual também utilizarmos a notação x $\longmapsto$ f(x) para indicarmos a aplicação f na qual f(x) é a imagem do elemento genérico x. O conjunto B será chamado de contradomínio de f.

Exemplos:

1) A relação R, de A = {1,2,3,5 } em B = {3,4,6,9 } representada por:



não é uma aplicação pois 2 $\notin$ D(f), como também 3R6 e 3R9.

2) Seja R a relação de equivalência em Q definida por (x,y) $\in$ R se e se somente se x – y $\in$ Z. R não é aplicação, pois, por exemplo, $\frac{5}{2}R\frac{1}{2}$ e $\frac{5}{2}R\frac{3}{2}$.

Definição: Dizemos que uma aplicação f : A $\rightarrow$ B é *injetora* quando elementos distintos de A tem imagens distintas em B, simbolicamente:

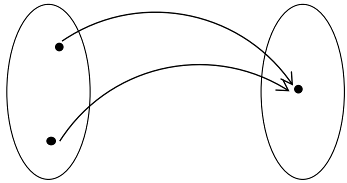
$$\forall(u,v)(u,v \in A \wedge u \neq v \rightarrow f(u) \neq f(v)),$$

ou seja, para todo u,v $\in$ A, se u $\neq$ v então f(u) $\neq$ f(v), que é o mesmo que:

$$\forall(u,v)(u,v \in A \wedge f(u) = f(v) \rightarrow u = v),$$

ou seja, para todo u,v $\in$ A, se f(u) = f(v) então u = v.

Nesta condição, em um diagrama de flechas, situações como a abaixo não são admitidas:



Assim, uma aplicação $f : A \to B$ não é injetora quando existem elementos distintos de A que tem a mesma imagem em B, simbolicamente:

$$\exists(u,v)(u,v \in A \wedge u \neq v \wedge f(u) = f(v)),$$

ou seja, existem $u,v \in A$, tais que $u \neq v$ e $f(u) = f(v)$.

Definição: Dizemos que uma aplicação $f : A \to B$ é *sobrejetora* quando $Im(f) = B$, simbolicamente:

$$\forall(y)(y \in B \to \exists(x)(x \in A \wedge y = f(x))),$$

ou seja, para todo $y \in B$ existe $x \in A$ tal que $y = f(x)$.

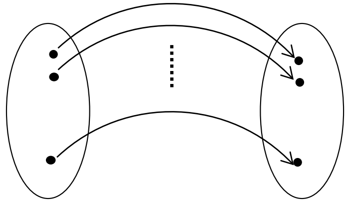
Nesta condição, em um diagrama de flechas, todo elemento de B é chegada de alguma flecha.

Por outro lado, uma aplicação $f : A \to B$ não é sobrejetora quando $Im(f) \neq B$, simbolicamente:

$$\exists(y)(y \in B \wedge \forall(x)(x \in A \wedge y \neq f(x))),$$

ou seja, existe $y \in B$ tal que para todo $x \in A$ tem-se $y \neq f(x)$, que é o mesmo que existe $y \in B$, tal que não existe $x \in A$ com $y = f(x)$.

Definição: Dizemos que uma aplicação $f : A \to B$ é *bijetora* se e somente se é injetora e sobrejetora. Em um diagrama de flechas temos a seguinte situação:



Dada uma aplicação $f : A \to B$, olhando - A apenas como uma relação de A em B sabemos que existe a relação inversa f^{-1}. No entanto, f^{-1} pode não ser uma aplicação de B em A. Vejamos um exemplo muito simples.

Exemplo: Sejam A = {1,2,3} e A = {5,6} e tomemos a aplicação f = {(1,5),(2,5),(3,6),(4,6)}. Neste caso f é uma aplicação mas a relação inversa f^{-1} = {(5,1),(5,2),(6,3),(6,4)} não é uma aplicação de B em A. Veja ainda que f é sobrejetora mas não é injetora.

Seja $f : A \to B$ uma aplicação de A em B. Uma condição necessária e suficiente para que a aplicação inversa f^{-1} exista é que f seja bijetora, ou seja, a aplicação f^{-1} existe se e somente se f é bijetora. Vamos demonstrar este resultado.

Suponhamos inicialmente que a aplicação f^{-1} existe. Daí:

a) f é injetora, pois se existem $u,v \in A$, tais que $y = f(u) = f(v)$ então $u = f^{-1}(y)$ e $v = f^{-1}(y)$ e como f^{-1} é aplicação temos que $f^{-1}(y)$ é único e portanto $u = v$.

b) f é sobrejetora, pois se $y \in b$, como f^{-1} é aplicação de B em A temos que existe $x \in A$ tal que $f^{-1}(y) = x$, e portanto, $y = f(x)$.

Logo f é bijetora.

Suponhamos agora que f é bijetora. Como f é sobrejetora para todo $y \in B$, existe $x \in A$ tal que $y = f(x)$ e portanto $(y,x) \in f^{-1}(x)$. Assim, $D(f^{-1}(x)) = B$. Agora, como f é injetora para todo $u,v \in A$, se $y = f(u) = f(v)$ então $u = v$, e assim se $(y,u) \in f^{-1}(x)$ e $(y,v) \in f^{-1}(x)$, então $u=v$, e, portanto, para todo $y \in B$ é único o elemento $x \in A$, tal que $(y,x) \in f^{-1}(x)$.

Logo f^{-1} é aplicação de B em A.

Definição: Seja A um conjunto não vazio. Uma *operação unitária* ou *singular* em A é uma aplicação:

$$\xi : A \to A$$
$$a \mapsto b,$$

a qual denotamos também por $\xi(a) = b$, onde $a,b \in A$.

Definição: Seja A um conjunto não vazio. Uma *operação binária* ou *lei de composição interna*, em A, é uma aplicação:

$$\varphi : AxA \to A$$
$$(a,b) \mapsto a \varphi b,$$

a qual denotamos também por $\varphi(a,b) = a\varphi b$, em que $a,b \in A$.

Exemplos:

1) $\xi : Z \to Z$

$z \mapsto -z,$

é uma operação unitária em A = Z.

2) $\xi: R \to R$

$x \mapsto |x|,$

é uma operação unitária em A = R.

3) $\varphi_1: NxN \to N$

$(m,n) \mapsto m + n,$

é uma operação binária em A = N.

4) $\varphi_2: NxN \to N$

$(m,n) \mapsto m \cdot n,$

é uma operação binária em A = N.

5) $\varphi_3: NxN \to N$

$(m,n) \mapsto m^n$

é uma operação binária em A = N.

Nos exemplos 3 e 4, se A = Z ou A = R, φ_1 e φ_2 ainda são operações binárias nesses conjuntos.

Observe que se A = Z, φ_3 não é uma operação binária nesse conjunto, pois nem sempre $\varphi_3(a,b) = a^b$ existe nesse conjunto. O mesmo vale se A = Z.

Quanto A é um conjunto finito, digamos com n elementos, podemos representar uma operação em A através de uma tabela ou tábua.

No caso das operações unitárias são necessárias duas colunas. Na primeira delas colocamos os elementos de A e na segunda os resultados obtidos para cada um desses elementos na operação. A primeira linha da tabela é usada para a identificação das colunas.

Exemplo: Seja A = (–3,–2,–1,1,2,3} e consideremos seja T a aplicação que troca o sinal de cada elemento de A. T é uma operação em A e sua tabela é:

A	T(A)
–3	3
–2	2
–1	1

1	–1
2	–2
3	–3

No caso das operações binárias, sendo A um conjunto finito com n elementos necessitamos de uma tabela com (n + 1) linhas e (n + 1) colunas. Preenchemos a linha inicial e a coluna inicial, ou linha zero e coluna zero, dessa tabela, a partir da segunda posição, com os elementos de A. Em seguida, na posição obtida pela interseção da linha i com a coluna j, anotamos o resultado da operação do i-ésimo elemento de A com o j-ésimo elemento de A, para $1 \leq i \leq n$ e $1 \leq j \leq n$.

Exemplos:

1) Considere $A = \{-1,0,1\}$. A tábua da operação multiplicação em A é:

·	–1	0	1
–1	1	0	–1
0	0	0	0
1	–1	0	1

2) Considere M = {1,3,5,15} e definamos a operação f por f(x,y) = mdc(x,y). A tábua desta operação em M é:

mdc	1	3	5	15
1	1	1	1	1
3	1	3	1	3
5	1	1	5	5
15	1	3	5	15

3) Considere o conjunto $E = \{f_1, f_2, f_3\}$ onde f_1, f_2 e f_3 são funções dadas por $f_1 = \{(a,a),(b,b),(c,c)\}$, $f_2 = \{(a,b),(b,c),(c,a)\}$

e $f_3 = \{(a,c),(b,a),(c,b)\}$. A tábua da operação de composição de funções em E é:

$\circ$	f_1	f_2	f_3
f_1	f_1	f_2	f_3
f_2	f_2	f_3	f_1
f_3	f_3	f_1	f_2

A partir deste ponto, quando mencionarmos apenas operação, estamos nos referindo a uma operação binária, visto que sobre as unitárias mais nada temos a estudar além de possíveis definições, enquanto que para as binárias ainda estudaremos as propriedades que estas podem ou não atender.

Definição: Seja $*$ uma operação num conjunto A. Dizemos que:

i) $*$ é *associativa* se para $\forall(a,b,c)(a,b,c \in A \rightarrow (a * b) * c = a * (b * c))$.

ii) $*$ é *comutativa* se para $\forall(a,b)(a,b \in A \rightarrow a * b = a * b)$.

iii) $*$ possui *elemento neutro* se existe um elemento $e \in A$ tal que para qualquer $a \in A$ temos que:

$a*e = a$, quando e é chamado de elemento neutro à direita,

$e*a = a$, quando é chamado de elemento neutro à esquerda.

iv) Se $*$ possui elemento neutro $e \in A$, todo $a \in A$ é *inversível*, *invertível* ou *simetrizável* na operação $*$, ou seja, existe $a' \in A$, chamado de inverso, oposto ou simétrico de a em relação à operação $*$, tal que:

$a*a' = e$, quando a' é chamado de inverso, oposto ou simétrico de a em relação à operação $*$ à direita,

$a'*a = e$, quando a' é chamado de inverso, oposto ou simétrico de a em relação à operação $*$ à esquerda.

Exemplos:

1) Consideremos a operação adição definida em N, denotada por +. Ela é associativa, comutativa e não possui elemento neutro.

2) Consideremos a operação adição definida em Z, denotada por +. Ela é associativa, comutativa, possui elemento neutro e = 0 (zero) e

todos os seus elementos são simetrizáveis e $a' = -a$ para qualquer $a \in Z$.

3) Em R a operação de adição é associativa, comutativa, possui elemento neutro $e = 0$ (zero) e todos os seus elementos são simetrizáveis sendo $a' = -a$ para qualquer $a \in R$.

4) Consideremos a operação multiplicação definida em N, denotada por $\cdot$. Ela é associativa, comutativa, possui elemento neutro $e = 1$, sendo este o único elemento inversível em N com $1' = 1$.

5) Consideremos a operação multiplicação definida em Z, denotada por $\cdot$. Ela é associativa, comutativa, possui elemento neutro $e = 1$ e os únicos elementos inversíveis são -1 e 1 com $1' = 1$ e $(-1)' = -1$.

6) Consideremos a operação multiplicação definida em R, denotada por $\cdot$. Ela é associativa, comutativa, possui elemento neutro $e = 1$ e qualquer $x \in R - \{0\}$ é inversível e seu inverso é $\frac{1}{x}$, pois $x \cdot \frac{1}{x} = \frac{1}{x} \cdot x = 1$.

Teorema: Seja $A \neq \{\ \}$ um conjunto e seja $*$ uma operação em A. Valem as seguintes afirmações:

i) Se $*$ possui elementos neutros $e_1 \in A$ e $e_2 \in A$ então $e_1 = e_2$, ou seja, se $*$ possui elemento neutro ele é único.

ii) Se $*$ possui elemento neutro $e \in A$, $*$ é associativa e a' e a'' são simétricos de $a \in A$ na operação $*$, então, $a' = a''$, ou seja, o simétrico de $a \in A$ é único.

iii) Se $*$ possui elemento neutro $e \in A$, $*$ é associativa e $a \in A$ tem simétrico $a' \in A$, então a' também tem simétrico e $(a')' = a$, ou seja, o simétrico do simétrico de $a \in A$ é o próprio $a \in A$.

iv) Se $*$ possui elemento neutro, $*$ é associativa, e se a e b são simetrizáveis em A na operação $*$, então $a * b$ também é simetrizável e $(a * b)' = b' * a'$.

Demonstração:

i) Como $e_2 \in A$ é elemento neutro, $e_1 * e_2 = e_1$, e como $e_1 \in A$ é elemento neutro $e_1 * e_2 = e_2$. Logo $e_1 = e_2$.

ii) $a' = a'*e = a'*(a*a'') = (a'*a) * a'' = e*a'' = a''$.

iii) Como a' é o simétrico de a, temos que $a*a' = a'*a = e$, e assim, temos que a' é simetrizável com simétrico a. De ii temos que tal simétrico é único. Logo podemos escrever $(a')' = a$.

iv) Veja que:

$(a*b)*(b'*a') = ((a*b)*b')*a' = (a*(b*b'))*a' = (a*e)*a' = a*a' = e$,

e que:

$(b'*a')*(a*b) = ((b'*a')*a)*b = (b'*(a'*a))*b = (b'*e)*b = b'*b = e$.

Logo $a*b$ é simetrizável e seu simétrico é $(a*b)' = b'*a'$, o que conclui a demonstração deste teorema.

As propriedades comutativa, elemento neutro e elementos simetrizáveis ou inversíveis podem ser facilmente verificadas nas tábuas das operações. Dada uma operação em um conjunto finito $A = \{a_1, a_2, \cdots, a_n\}$, a qual denotaremos por $*$, temos que:

- $*$ é comutativa se a sua tábua for simétrica em relação à diagonal principal, isto é, em relação aos elementos obtidos operando-se o i-ésimo elemento com ele próprio, para $1 \leq i \leq n$.
- $*$ possui elemento neutro desde que exista um elemento cuja linha e coluna são respectivamente a primeira linha e a primeira coluna da tabela. Assim a tábua terá o seguinte aspecto:

$*$	a_1	a_2	...	e	...	a_n
a_1				a_1		
a_2				a_2		
$\vdots$				$\vdots$		
e	a_1	a_2	...	e	...	a_n
$\vdots$				$\vdots$		
a_n				a_n		

- o í-ésimo elemento de A, ou seja, a_i, é simetrizável quando o elemento neutro figurar ao menos uma vez na linha i e na coluna i da tábua, ocupando posições simétricas em relação é diagonal principal.

$*$	a_1	a_2	...	a_i	...	a_j	...	a_n
a_1								
a_2								
$\vdots$								
a_i						e		
$\vdots$								
a_j				e				
$\vdots$								
a_n								

Veja que, na tábua anterior a_j é o simétrico de a_i pois:

$$a_i * a_j = e,$$
$$a_j * a_i = e,$$

e assim a localização de e na tábua determinará o simétrico de a_i.

7.5 Estruturas algébricas

Definição: Uma *estrutura algébrica* é um conjunto $A \neq \{\ \}$ juntamente com uma sequência finita de operações, unitárias ou binárias, em A, $*_1$, $*_2$, $\cdots$, $*_n$, com $n \geq 1$, a qual é usualmente denotada por uma (n+1)-upla:

$$(A, *_1, *_2, \cdots, *_n).$$

Como já afirmamos, em relação às operações unitárias nada além da definição da operação nos resta a estudar, visto que as propriedades operatórias são exclusivamente pertinentes às operações binárias. Por esse motivo, na classificação de uma estrutura algébrica, como veremos a seguir, apenas as operações binárias são consideradas, e lembramos que, como também já mencionado, quando mencionarmos apenas operação, estaremos nos referindo a uma operação binária.

Definição: Seja $A \neq \{\ \}$ e $*$ uma operação em A. A estrutura algébrica $(A,*)$ recebe o nome de:

1) *Semigrupo* se $*$ é associativa.

2) *Semigrupo* comutativo se $*$ é associativa e comutativa.

3) *Monoide* se $*$ é associativa e tem elemento neutro.

4) *Monoide comutativo* se $(A,*)$ é um monoide e $*$ é comutativa.

5) *Grupo* se $*$ é associativa, tem elemento neutro e todo elemento $a \in A$ é simetrizável na operação $*$.

6) *Grupo comutativo* ou *grupo abeliano* se $(A,*)$ é um grupo e $*$ é comutativa.

Observação: Quando afirmamos que $(A,*)$ é uma estrutura algébrica, estamos afirmando também que $*$ é uma operação, e assim A deve ser fechado em $*$, isto é, para qualquer $a,b \in A$, $a*b \in A$, o que deve ser preliminarmente verificado quando a operação $*$ for essencialmente nova, seja na sua definição ou na definição do seu domínio. Neste caso também dizemos que $*$ está bem definida em A.

Exemplos:

1) $(N,+)$ é um semigrupo comutativo.

2) $(N,\cdot)$ é um monoide comutativo.

3) $(Z,+)$ é um grupo abeliano.

4) $(Z,\cdot)$ é um monoide comutativo.

5) $(R,+)$ é um grupo abeliano.

6) $(R - \{0\},\cdot)$ é um grupo abeliano.

7) $(Q,+)$ é um monoide comutativo.

8) $(Q - \{0\},\cdot)$ é um grupo abeliano.

9) O conjunto $A = \{-3,-2,-1,0,1,2,3\}$ não é um grupo em relação à adição, embora 0 seja o elemento neutro, cada elemento de A tenha simétrico, e a adição seja associativa. A razão é que claramente a adição não é uma operação binária em A, uma vez que A não é fechado na operação adição, pois por exemplo $2 + 3 = 5 \notin A$.

10) Seja B um conjunto não vazio e seja:

$$A = \{f : B \to B | f \text{ é uma função}\}.$$

Seja "$\circ$" a operação de composição de funções, definida em A. $(A,\circ)$ é um monoide, mas esta operação não é comutativa se B tem ao menos 3 elementos.

Primeiramente observemos que a operação de composição de funções está bem definida em A, ou seja, é uma operação binária em A.

i) $\circ$ é associativa; pois para quaisquer f,g,h $\in$ A e qualquer b $\in$ B:

$((f\circ g)\circ h)(b) = (f\circ g)(h(b)) = f(g(h(b)))$,

$(f\circ(g\circ h)(b) = f((g\circ h)(b)) = f(g(h(b)))$.

ii) "$\circ$" possui elemento neutro, pois seja $I_B : B \to B$ a função identidade em B, isto é, $I_B(x) = x$ para todo x $\in$ B, pois para qualquer f $\in$ A e qualquer b $\in$ B:

$(f\circ I_B)(b) = f(I_B(b)) = f(b)$,

$(I_B\circ f)(b) = I_B(f(b)) = f(b)$.

Portanto (A,$\circ$) é um monoide.

iii) Suponhamos agora que B possui ao menos 3 elementos distintos dois a dois: a,b,c. Sejam f,g $\in$ A assim definidas:

$$\begin{cases} f(a) = b \\ f(b) = a \\ f(x) = x, \text{ se } x \in B - \{a, b\} \end{cases} \qquad \begin{cases} g(a) = c \\ g(c) = a \\ g(x) = x, \text{ se } x \in B - \{a, c\} \end{cases}$$

Veja que $(f\circ g)(b) = f(g(b)) = f(b) = a$ e $(g\circ f)(b) = g(f(b)) = g(a) = c$.

Logo, se B possui ao menos 3 elementos então (A,$\circ$) é um monoide não comutativo.

11) Seja K o conjunto das matrizes da forma $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, com a,b $\in$ R. Vamos mostrar que (K,+) é um grupo abeliano.

i) K é fechado em relação à +, pois sejam

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}, \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \in K$$

então:

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ -b-d & a+c \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ -(b+d) & a+c \end{pmatrix} = \begin{pmatrix} e & f \\ -f & e \end{pmatrix}$$

em que $\begin{cases} e = a + c \\ f = b + d \end{cases}$, e como a,c $\in$ R, e = a + c $\in$ R e como b,d $\in$ R, f = b + d $\in$ R, e assim $\begin{pmatrix} e & f \\ -f & e \end{pmatrix} \in K$.

ii) + associativa em K, pois sejam

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}, \begin{pmatrix} c & d \\ -d & c \end{pmatrix}, \begin{pmatrix} e & f \\ -f & e \end{pmatrix} \in K \text{ , então:}$$

$$\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \left(\begin{pmatrix} c & d \\ -d & c \end{pmatrix} + \begin{pmatrix} e & f \\ -f & e \end{pmatrix}\right)\right) = \left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c+e & d+f \\ -d-f & c+e \end{pmatrix}\right) =$$

$$= \begin{pmatrix} a+c+e & b+d+f \\ -b-d-f & a+c+e \end{pmatrix},$$

$$\left(\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix}\right) + \begin{pmatrix} e & f \\ -f & e \end{pmatrix}\right) = \left(\begin{pmatrix} a+c & b+d \\ -b-d & a+c \end{pmatrix} + \begin{pmatrix} e & f \\ -f & e \end{pmatrix}\right) =$$

$$= \begin{pmatrix} a+c+e & b+d+f \\ -b-d-f & a+c+e \end{pmatrix}$$

iii) + possui elemento neutro $e = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in K$, pois, para qualquer $\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in K$,

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a+0 & b+0 \\ -b+0 & a+0 \end{pmatrix} = \begin{pmatrix} a & b \\ -b & a \end{pmatrix},$$

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} 0+a & 0+b \\ 0+(-b) & 0+a \end{pmatrix} = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$

iv) Para qualquer $\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in K$, a matriz $\begin{pmatrix} -a & -b \\ b & -a \end{pmatrix} \in K$ e:

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} -a & -b \\ b & -a \end{pmatrix} = \begin{pmatrix} a+(-a) & b+(-b) \\ -b+b & a+(-a) \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = e,$$

$$\begin{pmatrix} -a & -b \\ b & -a \end{pmatrix} + \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} -a+a & -b+b \\ b+(-b) & -a+a \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = e$$

Assim qualquer matriz $\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in K$ é simetrizável e sua simétrica é $\begin{pmatrix} -a & -b \\ b & -a \end{pmatrix} \in K$.

v) + é comutativa em K, pois pra quaisquer $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}, \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \in K$, temos:

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ -b+(-d) & a+c \end{pmatrix} =$$

$$= \begin{pmatrix} c+a & d+b \\ -d+(-b) & c+a \end{pmatrix} = \begin{pmatrix} c & d \\ -d & c \end{pmatrix} + \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

Logo (K,+) é um grupo abeliano.

12) Sendo:

$$M_{mxn}(R) = \left\{ \begin{pmatrix} m_{11} & m_{12} & m_{13} & \cdots & m_{1n} \\ m_{21} & m_{22} & m_{23} & \cdots & m_{2n} \\ & & & \vdots & \\ m_{m1} & m_{m2} & m_{m3} & \cdots & m_{mn} \end{pmatrix} \middle| m_{ij} \in R, 1 \le i \le m, 1 \le j \le n \right\},$$

$(M_{mxn}(R),+)$ é um grupo abeliano e a demonstração é análoga ao exemplo anterior.

Seja (G,*) um grupo e seja m um número Inteiro positivo. Para qualquer $a \in G$, definimos:

$a^m = a*a* \cdots *a$, m fatores,

$a^0 = e$, o elemento neutro de G,

$a^{-m} = (a')^m = a'*a'*\cdots*a'$, m fatores, onde a' é o simétrico de a na operação *.

Veja que $(a^m)' = a^{-m}$, pois:

$$a^m * a^{-m} = \underbrace{(a * a * \cdots * a) * (a'*a'*\cdots * a')}_{\text{m fatores cada}} =$$

$$= \underbrace{(a * a * \cdots * a)}_{m-1 \text{ fatores}} * (a * a') * \underbrace{(a' * a' * \cdots * a')}_{m-1 \text{ fatores}} =$$

$$= \underbrace{(a * a * \cdots * a)}_{m-1 \text{ fatores}} * e * \underbrace{(a' * a' * \cdots * a')}_{m-1 \text{ fatores}} =$$

$$= \underbrace{(a * a * \cdots * a)}_{m-1 \text{ fatores}} * \underbrace{(a' * a' * \cdots * a')}_{m-1 \text{ fatores}} = \cdots = a * a' = e$$

e da mesma forma mostra-se que $a^{-m} * a^m = e$.

Observe que se $G = Q - \{0\}$ ou se $G = R - \{0\}$ e $* = \cdot$ então $e = 1$ e $a' = \frac{1}{a}$ e o definido acima recebe o nome de potência m-ésima de a e desta forma temos:

$a^m = a \cdot a \cdot \cdots \cdot a$, com m fatores,

$a^0 = 1$,

$a^{-m} = \frac{1}{a} \cdot \frac{1}{a} \cdot \cdots \cdot \frac{1}{a}$, com m fatores.

Quando $G = Z$ ou $G = Q$ ou $G = R$ e $* = +$ então $e = 0$ e $a' = -a$ e o definido acima recebe o nome de múltiplo de a e desta forma temos:

$a^m = m \cdot a = a + a + \cdots + a$, com m fatores,

$a^0 = 0 \cdot a = a$, o elemento neutro de G,

$a^{-m} = -m \cdot a = m \cdot (-a) = (-a) + (-a) + \cdots + (-a)$, com m fatores.

Teorema: Seja (G,*) um grupo. Para todo $a \in G$:

i) $a^m * a^n = a^{m+n}$,

ii) $(a^m)^n = a^{m \cdot n}$,

em que $m,n \in Z$.

Demonstração:

Consideremos primeiro que m e n são ambos positivos, isto é, $m > 0$ e $n > 0$:

$$a^m * a^n = \underbrace{(a * a * \cdots * a)}_{m \text{ fatores}} * \underbrace{(a * a * \cdots * a)}_{n \text{ fatores}} =$$

$$= \underbrace{(a * a * \cdots a * a)}_{m+1 \text{ fatores}} * \underbrace{(a * a * \cdots * a)}_{n-1 \text{ fatores}} =$$

$$= \underbrace{(a * a * \cdots a * a * \cdots a)}_{\text{m+n fatores}} = a^{m+n}$$

A demonstração de $(a^m)^n = a^{m \cdot n}$ neste caso é análoga à de $a^m * a^n = a^{m+n}$.

Consideremos primeiro que m e n tem sinais opostos, e escolhamos, $m < 0$ e $n > 0$:

Sejam $m = -r$ e $n = s$ em que r e s são inteiros positivos. Assim:

$$a^m * a^n = a^{-r} * a^s = (a')^r * a^s = \underbrace{(a' * a' * \cdots * a')}_{\text{r fatores}} * \underbrace{(a * a * \cdots * a)}_{\text{s fatores}} = \cdots =$$

$$\begin{cases} a^{s-r} = a^{m+n} \text{ se } s \geq r \\ (a')^{r-s} = a^{-(r-s)} = a^{s-r} = a^{m+n} \text{ se } s < r \end{cases}$$

A demonstração de $(a^m)^n = a^{m \cdot n}$ neste caso fica a cargo do leitor.

O caso $m < 0$ e $n < 0$ é análogo ao caso $m > 0$ e $n > 0$, e os casos em que $m = 0$ ou $n = 0$ são triviais.

Definição: Seja (G,*) um grupo. Qualquer subconjunto S de G é denominado um *subgrupo* de G se S é um grupo em relação à operação *.

Assim, se (G,*) é um grupo com elemento neutro e, sendo $S = \{e\}$ e $S = G$, temos que (S,*) são subgrupos de G. Eles são chamados de *subgrupos impróprios* de G. Outros subgrupos de G, se existirem, são chamados de *subgrupos próprios*.

Exemplos:

1) Considere o grupo (Z,+) e seja $Z^m = \{m \cdot z | z \in Z\}$ e m é um inteiro fixo. $(Z^m,+)$ é um subgrupo de (Z,+), pois:

+ é uma operação binária em Z^m, ou seja, Z^m é fechado na operação +, pois se $m \cdot z_1 \in Z^m$ e $m \cdot z_2 \in Z^m$ então:

$$m \cdot z_1 + m \cdot z_2 = m \cdot (z_1 + z_2) \in Z^m, \text{ pois } z_1 + z_2 \in Z.$$

Para quaisquer $m \cdot z_1 \in Z^m$, $m \cdot z_2 \in Z^m$ e $m \cdot z_3 \in Z^m$, temos:

$$(m \cdot z_1 + m \cdot z_2) = m \cdot z_3 = m \cdot (z_1 + z_2) + m \cdot z_3 = m \cdot ((z_1 + z_2) + z_3) =$$
$$= m \cdot (z_1 + (z_2 + z_3)) = m \cdot z_1 + m \cdot (z_2 + z_3) = m \cdot z_1 + (m \cdot z_2 + m \cdot z_3).$$

Logo + é associativa em Z^m.

$0 = m \cdot 0$ é o elemento neutro, pois para qualquer $m \cdot z \in Z^m$:

$$m \cdot 0 + m \cdot z = m \cdot (0 + z) = m \cdot z \text{ e}$$
$$m \cdot z + m \cdot 0 = m \cdot (z + 0) = m \cdot z.$$

Para qualquer $m \cdot z \in Z^m$, $m \cdot (-z) \in Z^m$ é o seu simétrico, pois:

$$m \cdot z + m \cdot (-z) = m \cdot (z - z) = m \cdot 0 \text{ e}$$
$$m \cdot (-z) + m \cdot z = m \cdot (-z + z) = m \cdot 0.$$

Logo $(Z^m,+)$ é um grupo e assim é um subgrupo de (Z,+).

2) Já verificamos que (K,+) é um grupo abeliano, e como K é um subconjunto de $M_2(R) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle\| a, b, c, d \in R \right\}$ temos que (K,+) é um subgrupo de $M_2(R)$.

A partir de agora trabalharemos estruturas algébricas com duas operações binárias, as quais, para facilitar a notação, denotaremos por "+" e "·", mas estas operações coincidem com a adição e a multiplicação usuais somente quando nada em contrário for definido.

Definição: Um conjunto não vazio A é um *anel* em relação às operações binárias + e ·, desde que, para arbitrários $a,b,c \in A$, as seguintes propriedades valem:

A1) $(a + b) + c = a + (b + c)$ (lei associativa da operação +);

A2) $a + b = b + a$ (lei comutativa da operação +);

A3) Existe $e \in A$ tal que $a + e = a$ (existência do elemento neutro da operação +);

A4) Para cada $a \in A$ existe $a' \in A$ tal que $a + a' = e$ (existência de simétricos na operação +);

A5) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (lei associativa da operação ·);

A6) $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ (lei distributiva à esquerda);

A7) $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ (lei distributiva à direita).

Notação: Em geral, se A é um anel em relação às operações + e · escrevemos (A,+,·) é um anel.

Exemplos:

1) (Z,+,·) é um anel.

2) (Q,+,·) é um anel.

3) (R,+,·) é um anel.

4) (C,+,·) é um anel, em que C representa o conjunto dos números Complexos.

5) $(M_n(R),+,\cdot)$ é um anel, em que $M_n(R)$ é o conjunto formado por todas as matrizes de números reais com n linhas e n colunas.

6) Sejam S o conjunto $S = \{a,b\}$, + a operação definida pela tábua:

+	a	b
a	a	b
b	b	a

e $\cdot$ a operação definida pela tábua:

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

Em primeiro lugar é óbvio que S é fechado em relação às operações + e $\cdot$.

A1) $(a + b) + a = b + a = b$,

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

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

Da mesma forma, verifica-se que vale esta propriedade para outras associações dos elementos de S, o que deixamos a cargo do leitor.

A2) $a + b = b$,

$b + a = b$

Logo, $a + b = b + a$.

A3) O elemento neutro é $e = a \in S$.

A4) O simétrico de cada $x \in S$ é o próprio x, pois:

$a + a = a = e$,

$b + b = a = e$.

A5) $(a \cdot b) \cdot a = a \cdot a = a$,

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

Logo $(a \cdot b) \cdot a = a \cdot (b \cdot a)$.

Da mesma forma, verifica-se que vale esta propriedade para outras associações dos elementos de S, o que deixamos a cargo do leitor.

A6) $a \cdot (b + a) = a \cdot b = a$,

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

Logo $a \cdot (b + a) = (a \cdot b) + (a \cdot a)$.

Da mesma forma verifica-se que vale esta propriedade pra outras disposições dos elementos de S, o que deixamos a cargo do leitor.

A7) Análoga à A6.

Logo $(S,+,\cdot)$ é um anel.

Observe que as operações + e $\cdot$ do último exemplo não tem qualquer significado fora das tabuas dadas.

Dado um anel $(A,+,\cdot)$ como $(A,+)$ é um grupo abeliano, vale que:

- O elemento neutro da operação + é único, o qual recebe o nome de elemento neutro aditivo;
- Cada elemento de A tem um único simétrico aditivo, isto é, na operação +;
- Se a' denota o simétrico de a na operação + em A então $(a')' = a$;
- $(a + b)' = b' + a'$ para todo $a,b \in A$.

Além disso, valem as seguintes propriedades:

P1) Leis do cancelamento para a operação +, ou seja, para todo $a,b,c \in A$:

Se $a + b = a + c$ então $b = c$ (lei do cancelamento à esquerda).

Demonstração:

Se $a + b = a + c$ então $a' + a + b = a' + a + c$ e assim $e + b = e + c$ em que concluímos que $b = c$, sendo que e denota o elemento neutro da operação + em A e a' denota o simétrico de a na operação + em A.

Se $a + b = c + b$ então $a = c$ (lei do cancelamento à direita).

Demonstração:

Se $a + b = c + b$ então $a + b + b' = c + b + b'$ e assim $a + e = c + e$ de onde concluímos que $a = c$, sendo que e denota o elemento neutro da operação + em A e b' denota o simétrico de b na operação + em A.

P2) Para qualquer $a \in A$,

$$a \cdot e = e \cdot a = e,$$

em que e é o elemento neutro da operação + em A.

Demonstração:

Observemos que como $a + e = a$ então:

$$a \cdot a = (a + e) \cdot a = (a \cdot a) + (e \cdot a).$$

Agora, $a \cdot a = (a \cdot a) + e$, portanto, $(a \cdot a) + (e \cdot a) = (a \cdot a) + e$, e daí, usando a lei do cancelamento à esquerda, temos $e \cdot a = e$.

Analogamente demonstra-se que $a \cdot e = e$.

P3) Para todo $a,b \in A$,

$$a \cdot b' = (a \cdot b)' = a' \cdot b,$$

em que a' denota o simétrico de a na operação + em A e b' denota o simétrico de b na operação + em A.

Demonstração:

Observemos que $(a \cdot b) + (a' \cdot b) = (a + a') \cdot b$ pela lei distributiva à direita. Assim,

$$(a \cdot b) + (a' \cdot b) = (a + a') \cdot b = e \cdot b = e,$$

pela propriedade P2, e denota o elemento neutro da operação + em A.

Também temos que $(a \cdot b) + (a \cdot b)' = e$.

Logo $(a \cdot b) + (a' \cdot b) = (a \cdot b) + (a \cdot b)'$ e pela lei do cancelamento à esquerda temos que:

$$a' \cdot b = (a \cdot b)'.$$

Analogamente se verifica que $a \cdot b' = (a \cdot b)'$ para assim concluirmos que:

$$a \cdot b' = (a \cdot b)' = a' \cdot b.$$

Definição: Seja $(A,+,\cdot)$ um anel. Qualquer subconjunto S de A é denominado um *subanel* de A se $(S,+,\cdot)$ é um anel.

Assim, se $(A,+,\cdot)$ é um anel com elemento neutro e para a operação +, sendo $S = \{e\}$ ou $S = A$, $(S,+,\cdot)$ são subanéis de A. Eles são chamados de *subanéis impróprios* de A. Outros subanéis de A, se existirem, serão chamados de *subanéis próprios*.

Definição: Seja $(A,+,\cdot)$ um anel. Dizemos que $(A,+,\cdot)$ é um *anel comutativo* se a operação $\cdot$ é comutativa, ou seja, para todo $a, b \in A$, $a \cdot b = b \cdot a$.

Exemplo: Os anéis dos últimos exemplos 1, 2, 3, 4 e 6 são comutativos. O anel do último exemplo 5 não é comutativo.

Definição: Seja (A,+,·) um anel. Dizemos que (A,+,·) é um *anel com unidade* se a operação · possui elemento neutro, que é chamado de elemento unidade.

Exemplo: Para os anéis dos exemplos 1, 2, 3 e 4 o elemento unidade é 1. Para o anel do exemplo 5 o elemento unidade é a matriz identidade com n linhas e n colunas e para o anel do exemplo 6 o elemento unidade é b.

Definição: Seja (A,+,·) um anel com elemento neutro e na operação +, e suponha que existe um inteiro positivo n tal que $n \cdot a = \underbrace{a + a + \cdots + a}_{\text{n fatores}} = e$ para todo a $\in$ A. O menor de tais inteiros positivos n recebe o nome de *característica* de A. Se nenhum tal inteiro existe, diz-se que A tem característica zero.

Exemplo: Os anéis (Z,+,·), (Q,+,·), (R,+,·) e (C,+,·) tem característica zero. Lembrando de Z_5 construído ao estudarmos a relação de congruência módulo m percebemos que (Z_5+,·) tem característica 5. (Z_{12},+,·) tem característica 12, e para começar a construí-lo basta pensar na horas em um relógio analógico.

Definição: Seja (A,+,·) um anel com elemento neutro e da operação +. Um elemento a $\in$ A, a $\neq$ e, é denominado um *divisor próprio de zero* se existe um elemento b $\in$ A, b $\neq$ e, tal que:

$$a \cdot b = e \text{ ou } b \cdot a = e.$$

Observe que o anel (M_n(R),+,·) possui divisores próprios de zero, visto que existem matrizes com n linhas e n colunas não nulas, que quando multiplicadas produzem a matriz nula como resultado, ou seja, o resultado da multiplicação é o elemento neutro da operação adição de M_n(R).

Definição: Seja (A,+,·) um anel comutativo e com unidade e seja e o elemento neutro da operação + em A. Se para todo a,b $\in$ A vale que se a · b = e então a = e ou b = e então (A,+,·) recebe o nome de *anel de integridade*.

Observe que um anel de integridade não possui divisores próprios de zero.

Exemplo: Os anéis (Z,+,·), (Q,+,·), (R,+,·) e (C,+,·) são anéis de integridade e assim não possuem divisores de zero. Em (Z_{12},+,·), $\overline{3}$ é um divisor de zero, pois $\overline{3} \cdot \overline{4} = \overline{12} = \overline{0}$.

Definição: Seja $(A,+,\cdot)$ um anel comutativo e com unidade u, e seja e o elemento neutro da operação + em A. Se todo $a \in A$, $a \neq e$ possui simétrico na operação $\cdot$ a estrutura $(A,+,\cdot)$ recebe o nome de *corpo*.

Exemplo: $(Q,+,\cdot)$, $(R,+,\cdot)$ e $(C,+,\cdot)$ são exemplos de corpos.

7.5.1 A álgebra Booleana

Agora apresentaremos a álgebra criada por George Boole, a álgebra Booleana, sobre a qual podemos dizer ser a pedra fundamental da informática. Como o leitor perceberá, a fundamentação teórica desta álgebra já nos é conhecida, seja estruturalmente, pelo que já apresentamos neste capítulo, como operacionalmente, pelo que estudamos no Cálculo Proposicional, o que será revisto, agora com uma nova rotulação, e assim sugerimos que um paralelo entre estes conteúdos e o Cálculo Proposicional seja estabelecido.

Definição: Uma *álgebra Booleana* é uma estrutura algébrica que contém duas operações binárias, as quais denotaremos por & e $\vee$, uma operação singular, a qual denotaremos por $\neg$, os elementos neutros das operações binárias $\vee$ e &, os quais denotaremos por 1 e 0 respectivamente, e recebem o nome de zero e elemento unidade, e um conjunto B, em que para todo $a,b,c \in B$, temos que valem as seguintes propriedades:

A1) $a \vee b = b \vee a$

A2) $a \,\&\, b = b \,\&\, a$

A3) $a \,\&\, (b \vee c) = (a \,\&\, b) \vee (a \,\&\, c)$

A4) $a \vee (b \,\&\, c) = (a \vee b) \,\&\, (a \vee c)$

A5) $a \vee 0 = a$

A6) $a \,\&\, 1 = a$

A7) $a \vee \neg a = 1$

A8) $a \,\&\, \neg a = 0$

A9) $0 \neq 1$

Observe que A1 e A2 são propriedades comutativas, A3 e A4 são propriedades distributivas, A5 e A6 caracterizam os elementos neutros e A7 e A8 caracterizam a complementação, conceitos já estudamos no Cálculo Proposicional e na Teoria dos Conjuntos.

Outros conceitos também já estudados, como fórmula, teorema, demonstrações, as considerações sobre parênteses, entre outros, devidamente adaptados à linguagem deste capítulo, devem ser aqui considerados, sempre que necessários.

Com a finalidade de esclarecimento denotamos uma álgebra Booleana por (B, &, $\vee$, $\neg$, 1, 0), ou seja, exibimos, além do conjunto B e das operações binárias, também a operação unitária e os elementos neutros das operações binárias.

Exemplo: Seja B = {1,2,5,7,10,14,35,70}ou seja, o conjunto dos divisores de 70. As operações são definidas como segue:

a & b será o mínimo múltiplo comum de a e b,

a $\vee$ b será o máximo divisor comum de a e b,

$\neg$a será 70 dividido por a,

para todo a,b $\in$ B.

Assim, neste conjunto com estas operações, temos que o elemento neutro de a & b = mmc(a,b) é 1 e o elemento neutro de a $\vee$ b = mdc(a,b) é 70.

Dessa maneira, a estrutura formada pelo conjunto B, pelas operações a & b = mmc(a,b), a $\vee$ b = mdc(a,b) e $\neg a = \frac{70}{a}$ e pelos elementos neutros 1 e 70, a qual representamos por $\left(B, \text{mmc}(a,b), \text{mdc}(a,b), \frac{70}{a}, 1, 70\right)$ é uma álgebra Booleana, na qual o zero da álgebra é 1, o elemento unidade da álgebra é 70. Abaixo apresentamos alguns exemplos de operações nessa estrutura:

5 & 14 = mmc(5,14) = 70

5 $\vee$ 14 = mdc(5,14) = 1

10 & 35 = mmc(10,35) = 70

10 $\vee$ 35 = mdc(10,35) = 5

$\neg 5 = \frac{70}{5} = 14$

$\neg 10 = \frac{70}{10} = 7$

Nota-se que podemos construir dessa maneira muitas álgebras Booleanas finitas. Em particular, uma álgebra Booleana muito conhecida e fundamental à computação é a álgebra Booleana mínima, ou álgebra dos computadores, ou álgebra dos zeros e uns, que é definida sobre o conjunto B = {0,1}. As operações &, $\vee$ e $\neg$ se comportam da seguinte maneira:

$$
\begin{array}{lll}
1 \,\&\, 1 = 1 & 1 \vee 1 = 1 & \\
1 \,\&\, 0 = 0 & 1 \vee 0 = 1 & \neg 0 = 1 \\
0 \,\&\, 1 = 0 & 0 \vee 1 = 1 & \neg 1 = 0 \\
0 \,\&\, 0 = 0 & 0 \vee 0 = 0 &
\end{array}
$$

E assim o elemento neutro da operação & é 1 e o elemento neutro de $\vee$ é 0.

Embora essa álgebra, como dissemos, seja conhecida como álgebra dos computadores, ela é a fundamental a todo processamento eletrônico, não apenas ao de dados. Veja que nela as operações &, $\vee$ e $\neg$ se comportam como a conjunção, a disjunção inclusiva e a negação respectivamente, e os elementos 0 e 1 como F e V respectivamente, do Cálculo Proposicional. Se preferir outra analogia, as operações &, $\vee$ e $\neg$ se comportam como a interseção, a união e a complementação respectivamente, e os elementos 0 e 1 como o conjunto vazio e o conjunto universo respectivamente, da Teoria dos Conjuntos.

Para uma álgebra Booleana qualquer (B,&,$\vee$,$\neg$,1,0) a terminologia é a seguinte:

a & b é chamado de encontro de a e b;

a $\vee$ b é chamado de junção de a e b;

$\neg$a é chamado de complemento de a.

A partir de agora apresentaremos alguns resultados e demonstrações pertinentes a qualquer álgebra Booleana (B,&,$\vee$,$\neg$,1,0), embora alguns já tenham sido por nós estudados. Agora eles tomarão a vestimenta própria desta álgebra, e principalmente, as demonstrações que apresentaremos têm agora o objetivo de nos familiarizar com esta nova linguagem.

Teorema da unicidade do complemento: Seja (B,&,$\vee$,$\neg$,1,0) uma álgebra Booleana qualquer. Se a $\vee$ b = 1 e a & b = 0, então, b = $\neg$a.

Demonstração: Observemos que:

b =

$= b \vee 0$ (A5)
$= b \vee (a \,\&\, \neg a)$ (A8)
$= (b \vee a) \,\&\, (b \vee \neg a)$ (A4)
$= (a \vee b) \,\&\, (b \vee \neg a)$ (A1)
$= 1 \,\&\, (b \vee \neg a)$ (hipótese)
$= (b \vee \neg a) \,\&\, 1$ (A2)
$= b \vee \neg a$ (A6),

e que:

$\neg a =$
$= \neg a \vee 0$ (A5)
$= \neg a \vee (a \,\&\, b)$ (hipótese)
$= (\neg a \vee a) \,\&\, (\neg a \vee b)$ (A4)
$= (a \vee \neg a) \,\&\, (\neg a \vee b)$ (A1)
$= 1 \,\&\, (\neg a \vee b)$ (A7)
$= (\neg a \vee b) \,\&\, 1$ (A2)
$= \neg a \vee b$ (A6)
$= b \vee \neg b$ (A1)

Logo $b = \neg a$.

Corolário: Seja $(B,\&,\vee,\neg,1,0)$ uma álgebra Booleana qualquer. Para todo a em B, temos:

$$\neg(\neg a) = a.$$

Adaptando o tópico sobre uso de parênteses do Cálculo Proposicional para a linguagem desta álgebra facilitaremos a notação, denotando $\neg(\neg a)$ por $\neg\neg a$.

Demonstração: Temos que:

$\neg a \vee a =$
$= a \vee \neg a$ (A1)
$= 1$(A7),

e que:

$\neg a \,\&\, a =$
$= a \,\&\, \neg a$ (A2)
$= 0$ (A8)

Assim, podemos aplicar o teorema anterior, tomando-se a como $\neg a$ e b como a, para obter $a = \neg\neg a$.

Teorema da idempotência: Seja $(B,\&,\vee,\neg,1,0)$ uma álgebra Booleana qualquer. Para todo a em B temos:

$$\text{i) } a \,\&\, a = a$$
$$\text{ii) } a \vee a = a$$

Demonstração:

i)

$a =$

$= a \,\&\, 1$ (A6)

$= a \,\&\, (a \vee a)$ (A7)

$= (a \,\&\, a) \vee (a \,\&\, a)$ (A3)

$= (a \,\&\, a) \vee 0$ (A8)

$= a \,\&\, a$ (A5)

ii)

$a =$

$= a \vee 0$ (A5)

$= a \vee (a \,\&\neg a)$ (A8)

$= (a \vee a) \,\&\, (a \vee \neg a)$ (A4)

$= (a \vee a) \,\&\, 1$ (A7)

$= a \vee a$ (A6)

Definição: Por *dual* de uma fórmula com respeito a uma álgebra Booleana qualquer $(B,\&,\vee,\neg,1,0)$, entenderemos a fórmula obtida pela substituição de & por $\vee$, $\vee$ por &, 1 por 0 e 0 por 1, isto é, trocando-se & e $\vee$ e trocando-se 0 e 1, uns pelos outros.

Exemplo: O dual de:

$$a \,\&\, (b \vee c) = (a \,\&\, b) \vee (a \,\&\, c)$$

é:

$$a \vee (b \,\&\, c) = (a \vee b) \,\&\, (a \vee c).$$

Exemplo: O dual de:

$$a \vee \neg a = 1$$

é:

$$a \,\&\, \neg a = 0.$$

É evidente que se A é o dual de B, então B é o dual de A.

Teorema do princípio da dualidade: Em uma álgebra Booleana qualquer $(B,\&,\vee,\neg,1,0)$, se uma fórmula A é dedutível das propriedades (1) - (9), então o dual de A também é dedutível das propriedades (1) - (9).

Demonstração: O dual de cada uma das propriedades (1) - (9) é também uma propriedade: (1) e (2) são duais uma da outra, e também o são os pares (3) e (4), (5) e (6) e (7) e (8), e (9) é dual dela mesma. Assim, se em uma demonstração de uma fórmula A trocamos cada fórmula por seu dual, o resultado continua sendo uma demonstração (já que propriedades são trocadas por propriedades), mas esta demonstração é agora uma demonstração do dual da fórmula A.

Teorema: Seja $(B,\&,\vee,\neg,1,0)$ uma álgebra Booleana qualquer. Para todo $a,b,c \in B$, temos:

i) $a \& a = 0$
ii) $a \vee 1 = 1$
iii) $a \& (a \vee b) = a$
iv) $a \vee (a \& b) = a$
v) Se $b \& a = c \& a$ e $b \& \neg a = c \& \neg a$, então, $b = c$
vi) $a \vee (b \vee c) = (a \vee b) \vee c$
vii) $a \& (b \& c) = (a \& b) \& c$
viii) $\neg(a \vee b) = \neg a \& \neg b$
ix) $\neg(a \& b) = \neg a \vee \neg b$
x) $a \vee b = \neg(\neg a \& \neg b)$
xi) $a \& b = \neg(\neg a \vee \neg b)$
xii) $a \& \neg b = 0$ se e somente se $a \& b = a$
xiii) $\neg 0 = 1$
xiv) $\neg 1 = 0$
xv) $a \& (\neg a \vee b) = a \& b$
xvi) $a \vee (\neg a \& b) = a \vee b$

Demonstração: Daqui para frente, fica a cargo do leitor identificar quais as propriedades e teoremas justificam cada passo da demonstração, e também, algumas passagens triviais serão omitidas.

i)
$a \& 0 =$
$= (a \& 0) \vee 0$
$= (a \& 0) \vee (a \& \neg a)$
$= (a \& \neg a) \vee (a \& 0)$
$= a \& (\neg a \vee 0)$
$= a \& \neg a$
$= 0.$

ii) é o dual de i.

iii)

$a \,\&\, (a \vee b) =$

$= (a \vee 0) \,\&\, (a \vee b)$

$= a \vee (0 \,\&\, b)$

$= a \vee (b \,\&\, 0)$

$= a \vee 0$ (i deste teorema)

$= a.$

iv) é o dual de iii.

v)

$b=$

$= b \,\&\, 1$

$= b \,\&\, (a \vee \neg a)$

$= (b \,\&\, a) \vee (b \,\&\, \neg a)$

$= (c \,\&\, a) \vee (c \,\&\, \neg a)$ (hipótese deste item)

$= c \,\&\, (a \vee \neg a)$

$= c \,\&\, 1$

$= c.$

vi) Usaremos v), trocando b por $(a \vee (b \vee c))$ e c por $((a \vee b) \vee c)$. Veja que para tanto apenas precisamos mostrar que:

a) $(a \vee (b \vee c)) \,\&\, a = ((a \vee b) \vee c) \,\&\, a$

b) $(a \vee (b \vee c)) \,\&\, \neg a = ((a \vee b) \vee c) \,\&\, \neg a$

Vamos mostrar a:

$(a \vee (b \vee c)) \,\&\, a =$

$= a \,\&\, (a \vee (b \vee c))$

$= a$ (iii deste teorema)

$((a \vee b) \vee c)) \,\&\, a =$

$= a \,\&\, ((a \vee b) \vee c)$

$= (a \,\&\, (a \vee b)) \vee (a \,\&\, c)$

$= a \vee (a \,\&\, c)$ (iii deste teorema)

$= a$ (iv deste teorema)

Assim $(a \vee (b \vee c)) \,\&\, a = ((a \vee b) \vee c) \,\&\, a$, demonstrando a.

Vamos mostrar b:

$(a \vee (b \vee c)) \,\&\, \neg a =$

$= \neg a \,\&\, (a \vee (b \vee c))$

$= (\neg a \,\&\, a) \vee (\neg a \,\&\, (b \vee c))$

$= 0 \vee (\neg a \,\&\, (b \vee c))$

$= \neg a \ \& \ (b \vee c)$

$((a \vee b) \vee c)) \ \& \ \neg a =$

$= \neg a \ \& \ ((a \vee b) \vee c) =$

$= (\neg a \ \& \ (a \vee b)) \vee (\neg a \ \& \ c)$

$= ((\neg a \ \& \ a) \vee (\neg a \ \& \ b)) \vee (\neg a \ \& \ c)$

$= (0 \vee (\neg a \ \& \ b)) \vee (\neg a \ \& \ c)$

$= \neg a \ \& \ (b \vee c)$

Assim $(a \vee (b \vee c)) \ \& \ \neg a = ((a \vee b) \vee c) \ \& \ \neg a$, demonstrando b.

vii) é o dual de vi.

viii) Para provarmos que $\neg(a \vee b) = \neg a \ \& \ \neg b$, usaremos o teorema da unicidade do complemento. Assim precisamos mostrar que:

$$(a \vee b) \ \& \ (\neg a \ \& \ \neg b) = 0 \text{ e } (a \vee b) \vee (\neg a \ \& \ \neg b) = 1,$$

Veja que:

$(a \vee b) \ \& \ (\neg a \ \& \ \neg b) =$

$= (\neg a \ \& \ \neg b) \ \& \ (a \vee b)$

$= ((\neg a \ \& \ \neg b) \ \& \ a) \vee ((\neg a \ \& \ \neg b) \ \& \ b)$

$= (a \ \& \ (\neg a \ \& \ \neg b)) \vee (a \ \& \ (\neg b \ \& \ b))$

$= ((a \ \& \ \neg a) \ \& \ \neg b) \vee (a \ \& \ (b \ \& \ \neg b))$

$= (0 \ \& \ \neg b) \vee (a \ \& \ 0)$

$= 0 \vee 0$

$= 0$

e:

$(a \vee b) \vee (\neg a \ \& \ \neg b) =$

$= ((a \vee b) \vee \neg a) \ \& \ ((a \vee b) \vee \neg b)$

$= (\neg a \vee (a \vee b) \ \& \ (a \vee (b \vee \neg b)$

$= ((\neg a \vee a) \vee b) \ \& \ (a \vee 1)$

$= ((a \vee \neg a) \vee b) \ \& \ 1$

$= (a \vee \neg a) \vee b$

$= 1 \vee b$

$= b \vee 1$

$= 1$

ix) é o dual de viii.

x) Por viii, $\neg(a \vee b) = \neg a \ \& \ \neg b$. Logo $\neg\neg(a \vee b) = \neg(\neg a \ \& \neg b)$. Mas $\neg\neg(a \vee b) = a \vee b$ pelo corolário do teorema da unicidade do complemento. Assim, $a \vee b = \neg(\neg a \ \& \ \neg b)$.

xi) é o dual de x.

xii)

$a =$

$= a \,\&\, 1$

$= a \,\&\, (b \vee \neg b)$

$= (a \,\&\, b) \vee (a \,\&\, \neg b).$

Portanto $a \,\&\, \neg b = 0$ implica $a = a \,\&\, b$.

Reciprocamente, suponhamos que $a = a \,\&\, b$. Então:

$a \,\&\, \neg b =$

$= 0 \vee (a \,\&\, \neg b)$

$= (a \,\&\, \neg a) \vee (a \,\&\, \neg b)$

$= a \,\&\, (\neg a \vee \neg b)$

$= a \,\&\, \neg(a \,\&\, b)$

$= a \,\&\, \neg a$ (hipótese $a = a \,\&\, b$)

$= 0$

xiii) Como $0 \vee 1 = 1$ e $0 \,\&\, 1 = 0$ obtemos $\neg 0 = 1$, pelo teorema da unicidade do complemento.

xiv) é o dual de xiii.

xv)

$a \,\&\, (\neg a \vee b) =$

$= (a \,\&\, \neg a) \vee (a \,\&\, b)$

$= 0 \vee (a \,\&\, b)$

$= a \,\&\, b$

xvi) é o dual de xv.

7.5.2 A base binária

Dado qualquer número natural $B \geq 2$, a notação:

$$a_n a_{n-1} \cdots a_2 a_1 a_0 a_{-1} a_{-2} \cdots$$

representa, na base B, o número:

$$a_n \cdot B^n + a_{n-1} \cdot B^{n-1} + \cdots + a_2 \cdot B^2 + a_1 \cdot B^1 + a_0 \cdot B^0 + a_{-1} \cdot B^{-1} + a_{-2} \cdot B^{-2} + \cdots$$

em que os coeficientes a_i são algarismos tais que $0 \leq a_i < B$. Cabe ressaltar que a exigência $a_i < B$ se faz presente para que essa representação seja única, pois caso contrário, admitindo $a_i \geq B$ temos, pelo algoritmo da divisão, que $a_i = k \cdot B + r$ com $k \geq 1$ e $0 \leq r < B$, daí:

$$a_n \cdot B^n + a_{n-1} \cdot B^{n-1} + \cdots + a_i \cdot B^i + \cdots$$
$$\cdots + a_2 \cdot B^2 + a_1 \cdot B^1 + a_0 \cdot B^0 + a_{-1} \cdot B^{-1} + a_{-2} \cdot B^{-2} + \cdots$$

é o mesmo que:

$$a_n \cdot B^n + a_{n-1} \cdot B^{n-1} + \cdots + (a_{i+1} + k) \cdot B^{i+1} + r \cdot B^i + \cdots$$
$$\cdots + a_2 \cdot B^2 + a_1 \cdot B^1 + a_0 \cdot B^0 + a_{-1} \cdot B^{-1} + a_{-2} \cdot B^{-2} + \cdots$$

e a exigência $a_i \geq 0$ também pode ser justificada por esse mesmo motivo.

A base que nos interessa é a base B = 2, chamada base binária, na qual computadores normalmente operam. Por exemplo, nessa base o número x = 1001.101 representa o número:

$$1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 + 1 \cdot 2^{-1} + 0 \cdot 2^{-2} + 1 \cdot 2^{-3}$$

ou seja, 9.625 na base decimal.

De modo geral, na base binária, base 2, a notação $a_n a_{n-1} \cdots a_2 a_1 a_0 a_{-1} a_{-2} \cdots$ de um número real qualquer representa:
$$a_n \cdot 2^n + a_{n-1} \cdot 2^{n-1} + \cdots + a_2 \cdot 2^2 + a_1 \cdot 2^1 + a_0 \cdot 2^0 + a_{-1} \cdot 2^{-1} + a_{-2} \cdot 2^{-2} + \cdots$$
com $a_i \in \{0,1\}$.

Dado um número real qualquer numa base B, podemos escrevê-lo em uma base B', a partir de adequação conveniente de seus coeficientes $a_i = 0,1,2,3,\cdots,B-1$ e de uma potência adequada na nova base B'. Nosso interesse neste texto é a mudança da base decimal, a que frequentemente usamos, para a base binária, a base utilizada no processamento eletrônico das informações.

Inicialmente consideremos o número inteiro $a_n a_{n-1} \cdots a_2 a_1 a_0$ na base 10, ou seja o número:

$$a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0 \cdot 10^0$$

o qual designaremos por n. O algoritmo da divisão nos diz que dados dois números inteiros n e d, com d > 0, existem dois números inteiros q e r, únicos, tais que $n = q \cdot d + r$, com $0 \leq r < d$. Sendo d = 2 e temos r = 0 ou r = 1.

Assim:

$$n = q \cdot 2 + r$$

e sendo q > 1, podemos escrever:

$$q = q_1 \cdot 2 + r_1$$

e assim sucessivamente obtemos:

$$q_1 = q_2 \cdot 2 + r_2$$
$$q_2 = q_3 \cdot 2 + r_3$$
$$\vdots$$

ou de forma geral:

$$q_i = q_{i+1} \cdot 2 + r_{i+1}$$

até obtermos $q_{i+1} = 1$, pois daí:

$$q_{i+1} = 0 \cdot 2 + r_{i+2} \text{ com } r_{i+2} = 1$$

e

$$0 = 0 \cdot 2 + 0$$

e a partir daí nenhuma novidade o algoritmo da divisão nos apresentará.

Daí:

$$n = q \cdot 2 + r = (q_1 \cdot 2 + r_1) \cdot 2 + r = q_1 \cdot 2^2 + 2^1 \cdot r_1 + 2^0 \cdot r = (q_2 \cdot 2 + r_2) \cdot 2^2 + 2^1 \cdot r_1 + 2^0 \cdot r = q_2 \cdot 2^3 + 2^2 \cdot r_2 + 2^1 \cdot r_1 + 2^0 \cdot r$$

e assim sucessivamente, para obter:

$$n = r_{i+2} \cdot 2^{i+2} + \cdots + r_3 \cdot 2^3 + 2^2 \cdot r_2 + 2^1 \cdot r_1 + 2^0 \cdot r$$
$$= 1 \cdot 2^{i+2} + \cdots + r_3 \cdot 2^3 + 2^2 \cdot r_2 + 2^1 \cdot r_1 + 2^0 \cdot r$$

e desta forma a representação do número n na base binária é $1r_{i+1} \cdots r_3 r_2 r_1 r$.

Este processo de conversão de um número inteiro n para a base decimal é conhecido como procedimento das divisões sucessivas, o qual, resumidamente, consiste na divisão do número n na base decimal sucessivamente por 2, armazenando, a cada passo j, o algarismo do resto r_j, até que o quociente da divisão seja igual a 0. O binário é constituído pelos coeficientes do resto da divisão, a partir do resto mais significativo r_{i+1} para o menos significativo r.

Exemplo: A representação do número 25 na base 2 é:

$$11001 = 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0$$

pois:

$25 = 12 \cdot 2 + 1$
$12 = 6 \cdot 2 + 0$
$6 = 3 \cdot 2 + 0$
$3 = 1 \cdot 2 + 1$ e
$1 = 0 \cdot 2 + 1$

e desta forma temos $r_4 = 1$, $r_3 = 1$, $r_2 = 0$, $r_1 = 0$ e $r = 1$.

Quando o número na base decimal possui somente a parte fracionária, a conversão para a base binária é realizada pelo procedimento das multiplicações sucessivas. Este procedimento é constituído dos seguintes passos:

a) Multiplicamos o número fracionário por 2.

b) Do resultado do passo a, a parte inteira é o primeiro dígito binário.

c) Do resultado do passo a, a parte fracionária é novamente multiplicada por 2.

d) O processo continua até que a parte fracionária seja nula.

Exemplo: A representação do número 0.1875 na base binária é:

$$0.0011 = 0 \cdot 2^{-1} + 0 \cdot 2^{-2} + 1 \cdot 2^{-3} + 1 \cdot 2^{-4} = \left(\frac{3}{16}\right)_{10},$$

assim obtida:

$0.1875 \cdot 2 = 0.375$ $\rightarrow$ parte fracionária: 0.375 parte inteira: 0,
$0.375 \cdot 2 = 0.75$ $\rightarrow$ parte fracionária: 0.75 parte inteira: 0,
$0.75 \cdot 2 = 1.5$ $\rightarrow$ parte fracionária: 0.5 parte inteira: 1,
$0.5 \cdot 2 = 1.0$ $\rightarrow$ parte fracionária: 0 parte inteira: 1.

Quando o número possui parte inteira e parte fracionária, não nulas, aplicam-se os dois procedimentos acima descritos. Dessa forma, o número 13.25 é representado na base decimal por 1101.01.

Neste capítulo não apresentaremos exercícios sobre álgebra Booleana, pois, com certeza, este conteúdo será retomado em muitas outras disciplinas da sua matriz curricular.

7.6 Exercícios propostos

1) Sendo A = {1,2,3,4,5} e B = {6,7,8,9} verifique se R = {(1,7),(3,8),(3,9),(5,6)} é uma relação de A em B e em caso afirmativo determine:

a) D(R)

b) Im(R)

c) R^{-1}

d) $D(R^{-1})$

e) $Im(R^{-1})$

2) Sejam A = B = Z. Considere

$$R = \{(x,y) \in NxN | x = y\}$$

Verifique se R é uma relação em Z e em caso afirmativo determine:

a) $D(R)$
b) $Im(R)$
c) R^{-1}
d) $D(R^{-1})$
e) $Im(R^{-1})$

3) Construir sobre o conjunto $E = \{a,b,c,d\}$ relações R_1, R_2 R_3 e R_4, tais que:
i) R_1 é somente reflexiva
ii) R_2 é somente reflexiva e simétrica
iii) R_3 é somente simétrica e transitiva
iv) R_4 é reflexiva, simétrica e transitiva

4) Seja S a seguinte relação:

$$S = \{(x,y) \in RxR|x - y \in Q\}$$

Mostre que S é uma relação de equivalência.

5) Seja A = R. Seja S uma relação em A definida por:

$$S = \{(x,y) \in AxA|x = y\}$$

Mostre que S é uma relação de equivalência.

6) Seja A = R e definamos a relação S em A por:

$$S = \{(x,y) \in AxA|x^2 = y^2\}$$

Mostre que S é uma relação de equivalência em A.

7) Em N considere a relação:

$$R = \{(a,b) \in NxN|a \geq b\}$$

Verifique se R é uma relação de equivalência em N.

8) Entre as relações dos exercícios 4, 5, 6 e 7, qual(is) é(são) antissimétrica(s)?

9) Seja A = R e seja S a relação em A, definida como no exercício 6. Determine todas as classes de equivalência de R e R \ S.

10) Verifique se as relações dadas nos exercícios 1 e 2 são aplicações de A em B, e em caso negativo, explique o(s) motivo(s).

11) Verifique se as relações dadas nos exercícios 4, 5, 6 e 7 são aplicações em A, e em caso negativo, explique o(s) motivo(s).

12) Sejam E = {a,b,c} e F = {a,b,c,d} e considere as relações:
a) R = {(a,a),(b,a),(c,a)}
b) S = {(a,a),(b,b),(c,c)}
c) T = {(a,a),(b,b)}
Verifique quais são aplicações. Quando sim, verifique se é injetora ou sobrejetora. É possível determinar uma aplicação de E em F bijetora? Por quê?

13) Sejam A = R e a aplicação $f : A \to A$ dada por $f(x) = 2 \cdot x$. Verifique se f é bijetora e em caso afirmativo determine f^{-1}.

14) Em cada caso abaixo, considere a operação * sobre E e verifique se a mesma é associativa, se é comutativa, se possui elemento neutro em E e determine os elementos de E que possuem simétricos nessa operação:

a) E = R* e $x * y = \dfrac{x}{y}$
b) E = N e x * y = min(x,y)
c) E = R e x * y = max(x,y)
d) E = Z e x * y = mdc(x,y)
e) E = N e x * y = mdc(x,y)
f) E = Z e x * y = mmc(x,y)
g) E = N e x * y = mmc(x,y)

15) Em cada caso abaixo, está definida uma operação em ZxZ. Verifique se a mesma é associativa, se é comutativa, se existe elemento neutro e determine os elementos simetrizáveis (inversíveis):
a) $(a,b) * (c,d) = (a \cdot c,0)$

b) (a,b) Δ (a,b) = (a + c,b + d)

16) Construa a tábua da operação de composição de funções em $E = \{f_1, f_2, f_3, f_4\}$ em que $f_1 = \begin{pmatrix} a & b & c & d \\ a & b & c & d \end{pmatrix}$, $f_2 = \begin{pmatrix} a & b & c & d \\ b & c & d & a \end{pmatrix}$, $f_3 = \begin{pmatrix} a & b & c & d \\ c & d & a & b \end{pmatrix}$ e $f_4 = \begin{pmatrix} a & b & c & d \\ d & a & b & c \end{pmatrix}$.

17) Sendo e = {a,b,c,d}, a partir de cada tábua a seguir verifique se $*$ é comutativa, se existe elemento neutro e quais elementos são simetrizáveis:

a)

*	a	b	c	d
a	c	d	a	b
b	d	c	b	a
c	a	b	c	d
d	b	a	d	c

b)

*	a	b	c	d
a	c	a	d	b
b	a	b	c	d
c	b	c	d	a
d	d	d	a	c

18) Mostre que $GL_2(R) = \{A \in M_2(R) | \det(A) \neq 0\}$, com a operação de multiplicação de matrizes é um grupo não abeliano. $(GL_2(R), \cdot)$ é um subgrupo de $M_2(R)$?

19) Mostre que $H = \left\{ \begin{pmatrix} \cos a & \operatorname{sen} a \\ -\operatorname{sen} a & \cos a \end{pmatrix} \middle| \, a \in \mathbb{R} \right\}$ com a operação $\cdot$, de multiplicação de matrizes, é um subgrupo de $M_2(\mathbb{R})$.

20) Construa a tábua para S_2, o conjunto de todas as permutações de 2 elementos e sendo $*$ a operação de composição de permutações verifique se $(S_2,*)$ é um grupo abeliano.

21) Seja G o conjunto das aplicações $f_{a,b}$: R $\rightarrow$ R da forma $f_{a,b}(x) = a \cdot x + b$, com a e b reais e $a \neq 0$. Mostre que $(G,\circ)$ é um grupo, mas não é um grupo abeliano, onde "$\circ$" é a operação de composição de funções.

22) Mostre que $(M_2(R),+,\cdot)$ é um anel. É comutativo?

BIBLIOGRAFIA

ABE, J. Minoro; SCALZITTI, Alexandre; SILVA FILHO, J. Inácio. Introdução à lógica para a ciência da computação. São Paulo: Arte e Ciência, 2001.

ALENCAR FILHO, Edgard de. **Iniciação à lógica matemática.** São Paulo: Nobel, 1995.

COPI, Irving Marmer. **Introdução à lógica.** 3. ed. São Paulo: Mestre Jou, l981.

CURY, Márcia Xavier. **Introdução à lógica.** São Paulo: Érica, 1996.

DAGHLIAN, Jacob. **Lógica e álgebra de Boole.** 3. ed. São Paulo: Atlas, 1990.

DOMINGUES, Hygino Hugueros, IEZZI, Gelson. **Álgebra moderna.** São Paulo: Atual, 1982.

HEGENBERG, Leônidas. **Lógica:** simbolização e dedução. São Paulo: EPU, 1975.

MATES, Benson. **Lógica elementar.** São Paulo: Ed. Nacional, l968.

MENDELSON, Elliott. Álgebra booleana e circuitos de chaveamento. São Paulo: McGraw-Hill, 1977.

MONTEIRO, L. H. Jacy. **Iniciação às estruturas algébricas.** São Paulo: Nobel, 1969.

PIRES, Augusto de Abreu. Uma axiomatização para o cálculo proposicional. **Revista de Estudos Universitários,** Sorocaba, v. 23, n. 1, 1997.

GABARITO

Gabarito dos exercícios propostos

1. Cálculo Proposicional

1)

i)

a) João é bom aluno ou é estudioso.

b) João é bom aluno e é estudioso.

c) João é bom aluno ou não é estudioso.

d) João não é bom aluno e não é estudioso.

e) Não é verdade que João não é bom aluno.

f) Se João é bom aluno então é estudioso.

g) João é bom aluno se e somente se é estudioso.

h) Não é verdade que João não é bom aluno e não é estudioso.

ii)

a) $p \wedge - q$

b) $q \vee p$

c) $p \rightarrow q$

d) $- (p \wedge q)$

e) $p \leftrightarrow q$

f) $- (- q)$

2) Nesta resolução foi considerado que reprovado é o oposto de aprovado, não existindo uma terceira opção.

a) João não é bom aluno ou não é estudioso.
b) João é bom aluno ou é estudioso.
c) João não é bom aluno e não é estudioso.
d) João é bom aluno e não é estudioso.
e) João é estudioso.

3)
a) $vl\ (p \wedge -q) = V$
b) $vl\ (p \vee -q) = V$
c) $vl(-p \wedge q) = F$
d) $vl\ (-p \wedge -q) = F$
e) $vl(-p x\vee -q) = V$
f) $vl(p \wedge (-p \vee q)) = F$
g) $vl(-p \rightarrow q) = V$
h) $vl(-q \rightarrow p) = V$
i) $vl(-p \leftrightarrow q) = V$

4)
a) $vl(p) = V$ ou $vl(p) = F$
b) $vl(p) = F$
c) $vl(p) = V$
d) $vl(p) = F$
e) $vl(p) = F$
f) $vl(p) = F$

5)
a) $vl(p) = F$ e $vl(q) = V$ ou $vl(p) = F$ e $vl(q) = F$
b) $vl(p) = V$ e $vl(q) = V$ ou $vl(p) = F$ e $vl(q) = F$
c) $vl(p) = V$ e $vl(q) = V$
d) $vl(p) = F$ e $vl(q) = V$

6)
a) $vl(p \wedge (-q \rightarrow (r \wedge p_0))) = F$
b) $vl((p \leftrightarrow q) \vee (q \rightarrow -p)) = V$

c) $vl((- p \vee r) \rightarrow (q \rightarrow p_0)) = V$
d) $vl(((p \rightarrow q) \wedge p) \rightarrow - p) = V$
e) $vl((p \rightarrow r) \vee q) = V$

7)
a) Antecedente: chuva continuar;
Consequente: o rio transbordar.
b) Antecedente: chave central desligada;
Consequente: falha na rede elétrica.
c) Antecedente: abacates maduros;
Consequente: cremoso e macio.
d) Antecedente: gato saudável;
Consequente: boa dieta.

8)
a)

p	q	...	$((p \vee q) \leftrightarrow (q \vee p))$
V	V		V
V	F		V
F	V		V
F	F		V

Tautologia

b)

p	q	...	$((p \: x\vee \: q) \wedge (- p \wedge - q))$
V	V		F
V	F		F
F	V		F
F	F		F

Contradição

c)

p	q	…	$(p \leftrightarrow (p \vee q))$
V	V		V
V	F		V
F	V		F
F	F		V

Contingência

d)

p	q	…	$(((p \rightarrow q) \wedge q) \rightarrow p)$
V	V		V
V	F		V
F	V		F
F	F		V

Contingência

e)

p	q	…	$((p \vee q) \rightarrow (- p \wedge - q))$
V	V		F
V	F		F
F	V		F
F	F		V

Contingência

f)

p	q	…	$(- p \rightarrow (p \text{ x}\vee q))$
V	V		V
V	F		V
F	V		V
F	F		F

Contingência

g)

p	q	…	$((p \text{ x}\vee q) \leftrightarrow (q \rightarrow p))$
V	V		F
V	F		V
F	V		F
F	F		F

Contingência

h)

p	…	$(p \leftrightarrow - p)$
V		F
F		F

Contradição

i)

p	q	r	…	$((p \wedge (q \vee r)) \leftrightarrow ((p \wedge q) \vee (p \wedge r)))$
V	V	V		V
V	V	F		V
V	F	V		V
V	F	F		V
F	F	F		V
F	F	V		V
F	V	F		V
F	V	V		V

Tautologia

j)

p	q	r	…	$((p \rightarrow q) \rightarrow ((p \rightarrow r) \rightarrow (p \rightarrow r)))$
V	V	V		V
V	V	F		V
V	F	V		V
V	F	F		V
F	F	F		V

F	F	V		V
F	V	F		V
F	V	V		V

Tautologia

k)

p	q	…	$(p \wedge - (p \text{ x}\vee q))$
V	V		V
V	F		F
F	V		F
F	F		F

Contingência

l)

p	q	…	$((p \text{ x}\vee q) \rightarrow (- q \rightarrow p))$
V	V		V
V	F		V
F	V		V
F	F		V

Tautologia

m)

p	q	…	$((p \rightarrow q) \leftrightarrow (- p \vee q))$
V	V		V
V	F		V
F	V		V
F	F		V

Tautologia

n)

p	q	…	$((p \rightarrow q) \rightarrow (- q \rightarrow - p))$
V	V		V
V	F		V
F	V		V
F	F		V

Tautologia

o)

p	q	r	…	$((p \rightarrow (q \ x\vee \ r)) \leftrightarrow (p \wedge q) \vee (p \rightarrow r)))$
V	V	V		F
V	V	F		V
V	F	V		V
V	F	F		V
F	F	F		V
F	F	V		V
F	V	F		V
F	V	V		V

Contingência

p)

p	q	…	$((p \rightarrow q) \leftrightarrow - (p \wedge - q))$
V	V		V
V	F		V
F	V		V
F	F		V

Tautologia

q)

p	q	…	$((p \wedge q) \rightarrow (- q \rightarrow - p))$
V	V		V
V	F		V
F	V		V

F	F		V

Tautologia

r)

p	q	...	$((q \leftrightarrow (q \rightarrow p)) \rightarrow p)$
V	V		V
V	F		V
F	V		V
F	F		V

Tautologia

9)

a) $(p \leftrightarrow - p)$ é contradição.

b) $((p \rightarrow q) \rightarrow (- q \rightarrow - p))$ é tautologia.

c) $((p \wedge q) \rightarrow (- q \rightarrow - p))$ é tautologia.

d) $((p \text{ x}\vee q) \wedge (- p \wedge - q))$ é contradição.

10)

a) $(p \wedge (p \vee q))$ eq p

b) não ocorre nada.

c) $((p \wedge (p \rightarrow q)) \vdash q$

d) $(p \vee (p \wedge q))$ eq p

e) $p \vdash ((p \rightarrow q) \rightarrow q)$

f) $(p \rightarrow q)$ eq $(- p \vee q)$

g) $(p \rightarrow q) \vdash ((q \rightarrow r) \rightarrow (p \rightarrow r))$

h) $(p \leftrightarrow q)$ eq $((p \wedge q) \vee (- p \wedge - q)$

i) $(p \rightarrow q)$ eq $((- p \rightarrow q) \rightarrow q)$

j) $(q \rightarrow p)$ eq $(- q \vee p)$

k) $(p \vee (q \vee r))$ eq $((q \vee (p \vee r)) \vee p)$

l) $(p \rightarrow q)$ eq $- (p \wedge - q)$

m) $(p \vee q)$ eq $(- p \rightarrow q)$

n) $((p \wedge (p \rightarrow q))) \vdash q$

o) $((p \text{ x}\vee q) \wedge - q) \vdash p$

p) $(p \leftrightarrow q)$ eq $(q \leftrightarrow p)$

q) $(p \leftrightarrow q)$ eq $(- p \leftrightarrow - q)$

r) $(p \vee q)$ eq $- (- p \wedge - q)$

s) $(p \wedge q)$ eq $- (- p \vee - q)$

2. Construção e simplificação de fórmulas e formas normais

1)
p.

2)
q.

3)
a) Tautologia.
b) Tautologia.
c) Contingência.
d) Tautologia.
e) Tautologia.
f) Contradição.
g) Contingência.
h) Contradição.
i) Contradição.

3. Regras de inferência ou regras de dedução

1)
a)

(4) - C	MP 1, 2
(5) A	MP 3, 4

b)

(4) - A	MP 1, 2
(5) C	MP 3, 4

c)

(4) C	MP 2, 3
(5) - - C	DN 4
(6) - A	MT 1, 5

d)

(3) B	S1
(4) A	MP 2,3
(5) $B \wedge A$	A3, 4

e)

(4) C	S 1
(5) B	MP 3, 4
(6) $- - B$	DN 5
(7) $B \vee A$	CL 2
(8) A	TP 6, 7

f)

(5) $C \vee C$	DS 1, 2, 3
(6) C	LI 5
(7) $C \wedge (A \vee B)$	A 1, 6

g)

(5) $A \rightarrow - C$	HS 1, 2
(6) $- - C$	DN 3
(7) $- A$	MT 5, 6
(8) $E \wedge D$	TP 4, 7
(9) $D \wedge E$	CL 8
(10) D	S 9

h)

(3) $- D \wedge - - C$	DL 2
(4) $- - C$	S 3
(5) $(- C \rightarrow B \vee A - C) \wedge (B \vee A \rightarrow - C)$	LB 1
(6) $B \vee A \rightarrow - C$	S 5
(7) $- (B \vee A)$	MT 4, 6
(8) $- B \wedge - A$	DL 7
(9) $- A \wedge - B$	CL 8

32)

a) Consistente.

b) Consistente.

c) Inconsistente.

d) Consistente.

e) Inconsistente.

4. Cálculo de Quantificadores

1)

a) $\forall(x)(E(x) \rightarrow I(x))$

b) $\exists(x)(I(x) \wedge E(x) \wedge M(x))$

c) $\forall(x)(M(x) \rightarrow E(x))$

d) $\forall(x)(M(x) \rightarrow E(x) \wedge I(x))$

2) Veja que a fórmula dada significa "existe um inteiro positivo tal que todo inteiro menor que ele é não positivo". Seja $x = 1$, então, x é positivo e qualquer inteiro x_0 menor do que x é menor ou igual a zero, de modo que o valor lógico da proposição é verdade. Para a segunda interpretação, suponha que A(x) significa que "x é par", $B(x,x_0)$ que "$x < x_0$" e $C(x_0)$ que "x_0 é ímpar", a afirmação é falsa porque não existe um inteiro par com a propriedade de que todos os inteiros maiores são ímpares.

3)

a) Sejam:

F(x) representando "x é um número par";

a representando "10";

M(x) representando "x é múltiplo de 2".

Assim F(a) traduzirá "10 é um número par" e M(a) significará "10 é múltiplo de 2".

O argumento pode ser formalizado da seguinte maneira:

$$\begin{array}{c} \forall(x)(F(x) \rightarrow M(x)) \\ F(a) \\ \hline M(a) \end{array}$$

Note que foi usada a regra de inferência *Modus Ponens*, também foi feita a substituição da variável individual x, pela constante individual a que significava "10", nas letras funcionais F e M, que tinham as duas a mesma variável.

b) Sejam:

$D(x_1,x_2)$ representando "x_1 é divisor de x_2";

a_1 representando "10";

a_2 representando "20";

a_3 representando "5".

Assim $D(a_3,a_1)$ representará “5 é divisor de 10” e $D(a_3,a_2)$ representará “5 é divisor de 20”.

O argumento pode ser formalizado da seguinte maneira:

$$\frac{\begin{array}{c}\forall(x_1)(D(x_1,a_1) \rightarrow D(x_1,a_2)) \\ D(a_3,a_1)\end{array}}{D(a_3,a_2)}$$

A regra de inferência usada foi *Modus Ponens*, e também foi feita a substituição da variável individual x_1 pela constante individual a_3 que significava “5”.

c) Sejam:

A(x) representando “x é um ator”;

a representando “Augusto”;

R(x) representando “x gosta de representar”.

Assim, A(a) traduzirá “Augusto é um ator” e desta forma - A(a) traduzirá “Augusto não é um ator”, e R(a) significará “Augusto gosta de representar” implicando que - R(a) significará “Augusto não gosta de representar”.

O argumento pode ser formalizado da seguinte maneira:

$$\frac{\begin{array}{c}\forall(x)(A(x) \rightarrow R(x)) \\ -R(a)\end{array}}{-A(a)}$$

Note que foi usada a regra de inferência *Modus Tollens*. Também foi feita a substituição da variável individual x, pela constante individual a que significava “Augusto”, nas letras de predicados A e R, que tinham as duas a mesma variável.

5. Introdução à Teoria dos Conjuntos

1) Não.

2) Todos.

3) Os conjuntos dos itens a, b e c.

4) Nenhum.

5) Os conjuntos X e Y.

6) A afirmação do item a é verdadeira e a do item b é falsa.

7) Observe que 3 pertence a A, mas 3 não pertence a B.

8)

$$P(A) = \{\{1\},\{2\},\{3\},\{4\},\{1,2\},\{1,3\},\{1,4\},\{2,3\},\{2,4\},\{3,4\},$$
$$\{1,2,3\},\{1,2,4\},\{1,3,4\},\{2,3,4\},A,\{\,\}\}$$

$$P(B) = \{\{1\},\{2,3\},\{4\},\{1,\{2,3\}\},\{1,4\},\{\{2,3\},4\}, B\{\,\}\}.$$

9)
a) $X = C$ ou $X = E$
b) $X = D$ ou $X = E$
c) $X = A$ ou $X = B$ ou $X = D$.

10)
a) $Y \subseteq X$ é verdadeira.
b) $W \neq Z$ é verdadeira.
c) $Z \supseteq V$ é verdadeira.
d) $V \subseteq X$ é falsa.
e) $X = W$ é falsa.
f) $W \subseteq Y$ é falsa.

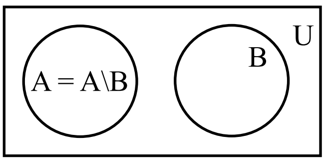
11)
a) $A \cup C = \{a,b,c,d,e,f,g\}$
b) $B \cap A = \{a,c,e\}$
c) $C \setminus B = \{b,f\}$
d) $B^C \cup C = \{b,d,e,f,g\}$
e) $C^C \cap A = \{a,c,d\}$
f) $(A \setminus C)^C = \{b,e,f,g\}$
g) $(A \setminus B^C)^C = \{b,d,f,g\}$
h) $(A \cap A^C)^C = U$

12)

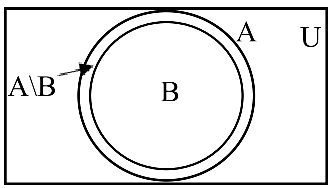
a) $(A^C \cap B^C)^C$
b) $(A^C \cup B^C)^C$

13)
a) $A^C = \{5,6,7,8,9\}$
b) $A \cap C = \{3,4\}$
c) $(A \cap C)^C = \{1,2,5,6,7,8,9\}$
d) $A \cup B = \{1,2,3,4,6,8\}$
e) $B \setminus C = \{2,8\}$

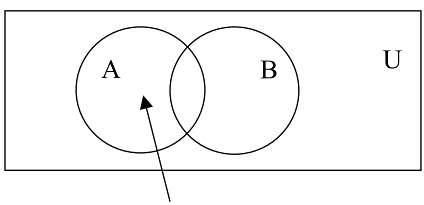
14)
a)



b)



c)



A\B

6. Álgebra Superior e álgebra Booleana

1)
R é uma relação, pois $R \subset AxB$.
a) $D(R) = \{1,3,5\}$
b) $Im(R) = B$
c) $R^{-1} = \{(7,1),(8,3),(9,3),(6,5)\}$
d) $D(R^{-1}) = B$
e) $Im(R^{-1}) = \{1,3,5\}$

2)
R é uma relação, pois $R \subset ZxZ$.
a) $D(R) = Z$
b) $Im(R) = Z$
c) $R^{-1} = R$
d) $D(R^{-1}) = Z$
e) $Im(R^{-1}) = Z$

3)
i) $R_1 = \{(a,a),(b,b),(c,c),(d,d),(a,b),(b,c),(c,b)\}$
ii) $R_2 = \{(a,a),(b,b),(c,c),(d,d),(a,b),(b,a),(b,c),(c,b)\}$
iii) $R_3 = \{(a,b),(b,a),(a,a),(b,b)\}$
iv) $R_4 = ExE$
Outras respostas são possíveis.

7) R não é relação de equivalência.

8) A relação R do exercício 7 e a relação R do exercício 9.

9)
$\overline{0} = \{0\}$ e para qualquer $x \in R^*$ temos que $\overline{x} = \{x,-x\}$ e
$R \backslash S = \{\{0\}, \{x\} | x \in R^*\}$.

10)
1) R não é aplicação pois $D(R) \neq A$ e 3R8 e 3R9.
2) R não é aplicação pois, por exemplo, 1R2 e 1R3.

3) R é aplicação.

11)

A relação do exercício 6 não é aplicação, pois, por exemplo, $\frac{5}{2}R1$ e $\frac{5}{2}R2$.

A relação do exercício 7 é aplicação.

A relação do exercício 8 não é aplicação pois por exemplo $1S-1$ e $1S1$.

A relação do exercício 9 não é aplicação pois por exemplo 1R1 e 1R2.

12)

R e S são aplicações. S é injetora. Não é possível determinar uma aplicação bijetora de E em F pois o número de elementos de E é diferente do número de elementos de F.

13)

f é bijetora e $f^{-1}(x) = \frac{x}{2}$.

14)

a) Nenhuma.

b) Associativa, comutativa.

c) Associativa, comutativa.

d) Associativa, comutativa.

e) Associativa, comutativa.

f) Associativa, comutativa.

g) Associativa, comutativa.

15)

a) Associativa, comutativa.

b) Associativa, comutativa, elemento neutro: (0,0). Elementos simetrizáveis: $\{(x,y)|x,y \in Z\}$.

16)

$\circ$	f_1	f_2	f_3	f_4
f_1	f_1	f_2	f_3	f_4
f_2	f_2	f_3	f_4	f_1
f_3	f_3	f_4	f_1	f_2
f_4	f_4	f_1	f_2	f_3

17)

a) $*$ é comutativa, possui elemento neutro c e os elementos simetrizáveis são a, b d.

b) O elemento neutro é b e o único elemento simetrizável é b.

20)

Seja $S_2 = (\alpha_0, \alpha_1\}$ em que $\alpha_0 = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$ e $\alpha_1 = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$. Temos que:

$$\alpha_0 * \alpha_1 = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} * \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = \alpha_1$$

$$\alpha_1 * \alpha_0 = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} * \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = \alpha_1$$

$$\alpha_1 * \alpha_1 = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} * \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} = \alpha_0$$

$$\alpha_0 * \alpha_0 = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} * \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} = \alpha_0$$

Logo a tábua solicitada é:

$*$	α_0	α_1
α_0	α_0	α_1
α_1	α_1	α_0

$(S_2, *)$ é um grupo, pois $*$ é associativa, α_0 é o elemento neutro e $\alpha_0' = \alpha_0$, $\alpha_1' = \alpha_1$. Como $\alpha_0 * \alpha_1 = \alpha_1 * \alpha_0$ temos que $(S_2,*)$ é grupo abeliano.

EDUNISO
Série Universitária

Missão da Universidade de Sorocaba

Ser uma Universidade Comunitária que, por meio da integração de ensino, pesquisa e extensão, produza conhecimentos e forme profissionais, em Sorocaba e região, para serem agentes de mudanças sociais, à luz de princípios cristãos.

UNISO (Filiada à Associação Brasileira das Universidades Comunitárias – ABRUC)

www.uniso.br