

Da contagem ao contínuo: uso e construção dos números reais

por António Bivar

Partindo das operações primitivas de contagem e medida, procurar-se-á conduzir os estudantes ao (re)conhecimento empírico dos diferentes conjuntos de números associados a essas operações e à compreensão dos problemas que o respectivo uso foi colocando ao pensamento matemático ao longo dos milénios, até se chegar às formalizações dos séculos XIX e XX. O objectivo fundamental será suscitar a necessidade de proceder a uma tal construção formalizada e revelar como esta nos permite encadear algumas das áreas mais abstractas dos fundamentos da Matemática com as estruturas algébricas elementares e as bases da análise real, integrando o conhecimento progressivo dos conjuntos numéricos que os estudantes foram adquirindo ao longo do percurso escolar.

1. Origem das operações de contagem e medida de grandezas; números inteiros e fracções racionais. Segmentos incomensuráveis: insuficiência dos números racionais. Números negativos.

Nem todas as comunidades humanas tiveram necessidade de recorrer à operação que designamos por “contagem”; ainda hoje, alguns grupos de caçadores e recolectores dispensam o uso dos números superiores a dois ou três. No entanto, pelo menos nos grupos em que se desenvolveu a actividade pastorícia, terá surgido naturalmente a ideia de controlar os efectivos, de modo a garantir a integridade dos rebanhos ou a acompanhar o respectivo aumento; um simples traço numa tábua ou uma pequena pedra¹ lançada num saco por cada animal que entra no recinto de recolha constitui um registo que pode ser utilizado no futuro para controlar, por exemplo, a falta de algum animal. A utilidade destes processos resulta muito simplesmente da maior facilidade de se garantir a inviolabilidade do suporte dos riscos ou do saco de pedras relativamente ao próprio rebanho, para além da possibilidade de se fazer indefinidamente “cópias” deste tipo de registos, em suportes de diversos tipos e transmiti-los a terceiros... As correspondências “um a um” assim estabelecidas (o que designamos por *correspondências biunívocas*), terão conduzido ao conceito intuitivo de *número inteiro* (etimologicamente “intocado”). De entre os inúmeros conjuntos-padrão que se podem utilizar destacam-se os que utilizam a própria anatomia humana, como sejam os dedos, os braços, as pernas, etc.; a forma como ainda hoje utilizamos os “números” guarda fortes reminiscências destes processos primitivos de contagem, a começar pela escolha da base decimal para a representação numérica. Nas diversas línguas faladas por algumas comunidades humanas estabeleceram-se sequências de palavras (orais e eventualmente escritas) precisamente destinadas a substituir os suportes materiais utilizados para a contagem; a memorização dessas sequências permitia dispensar os referidos suportes materiais e deste modo uma única palavra (simples ou composta) permitia reconstituir em qualquer momento

¹A palavra latina “calculus” (plural “calculi”) que significa exactamente “pequena pedra” está na origem dos termos “cálculo”, “calcular”, etc., utilizados em Matemática. De modo análogo o verbo “contar” provém do latim “computare” (derivado do verbo “putare” que significa considerar, avaliar, dando origem, por exemplo, ao verbo português “reputar” e ao substantivo “reputação”) que também deu origem às “contas” dos colares, outro possível instrumento de “controle de efectivos”.

uma correspondência biunívoca determinada, destinada a testar a integridade de determinado património ou a avaliar determinado conjunto de mercadorias.

Fixemos para já a estreita ligação que fica claramente estabelecida entre os conceitos básicos de contagem e de número inteiro, por um lado, e a consideração de colecções de objectos entre as quais se estabelecem correspondências um a um, por outro. A possibilidade de reunir os objectos de diversos conjuntos para formar novas colecções e a ideia de constituir novos conjuntos por emparelhamento de objectos retirados de determinadas colecções (como se faz, por exemplo, quando se estabelecem correspondências um-a-um) têm contrapartida nas operações de contagem, conduzindo às diversas operações sobre números inteiros.

A actividade agrícola, por um lado intimamente ligada às variações climatéricas e por outro conduzindo naturalmente a uma delimitação progressivamente mais rigorosa dos terrenos, levou a uma utilização mais sofisticada da contagem; entrou em cena a avaliação do tempo e do espaço. Tornou-se imprescindível contar os dias que regulam os ciclos das estações, contar meses e anos, ou seja, contar as fases da Lua, controlar os movimentos do Sol relativamente às estrelas e a outros pontos de referência, registar os conhecimentos adquiridos e transmiti-los de geração em geração. Se a contagem dos dias pouco mais exige que a contagem de ovelhas – sendo de notar que apesar de tudo a “calendarização” das estações do ano implica uma utilização mais intensa da memória ou de registos escritos – já a avaliação das posições relativas dos astros ou das extensões dos terrenos agrícolas envolve novos conceitos; a posição dos nossos olhos e dois pontos suficientemente distantes para que não seja relevante a visão estereográfica (resultante do afastamento entre os olhos) determinam o que se designa por um *ângulo* (com *vértice* nos olhos) que pode servir de padrão para avaliar a posição relativa de outros dois pontos também distantes. Podemos deslocar o ângulo padrão e *justapô-lo “extremidade a extremidade”* certo número de vezes de modo a procurarmos “*preencher exactamente*” o ângulo determinado pelos outros dois pontos, pelo que uma operação de contagem, utilizando as propriedades da nossa visão, pode em certos casos permitir avaliar, por exemplo, as posições relativas do Sol poente e de um ponto no horizonte, para determinado observador. No entanto, não é difícil concluir que só em casos raros uma simples contagem como esta servirá os nossos propósitos; muitas vezes será necessário alterar o padrão escolhido e procurar outro mais “refinado”, esperando que o novo padrão “caiba” certo número de vezes no inicialmente escolhido e preencha agora com rigor razoável o ângulo a medir por justaposição sucessiva um número “certo” de vezes. Desta maneira, com duas contagens após eventualmente algumas tentativas, podemos referenciar a posição relativa aparente de dois pontos para determinado observador, ou seja, por outras palavras, *medir* a respectiva distância angular, o que pode servir, por exemplo, para determinar se o Sol poente está na posição correspondente a determinado dia do ano propício ao início de certa operação agrícola. Utilizando segmentos em lugar de ângulos podem efectuar-se operações semelhantes para “medir” distâncias lineares e posteriormente avaliar áreas e volumes.

Pensou-se até há cerca de dois mil e quinhentos anos (tanto quanto se sabe) que as operações de contagem e medição do tipo das atrás esboçadas esgotavam as

possibilidades existentes no âmbito da medida de grandezas; por outras palavras, dadas duas quaisquer “grandezas da mesma espécie” seria sempre possível tomar uma delas para unidade e encontrar dois números inteiros p e q tais que a segunda grandeza se pudesse exprimir na unidade escolhida através de uma sequência de operações como as atrás descritas, correspondentes a estes dois números. Mais precisamente, seria possível encontrar uma nova unidade que reproduzisse a primitiva através de exactamente q justaposições e reproduzisse a grandeza a medir através de p justaposições; a nova unidade é o que representamos hoje por $1/q$ da primitiva, dizendo-se então que a medida obtida em termos da unidade inicial é p/q ⁽²⁾. Fica por definir qual o processo exacto de “justapor extremo a extremo certo número de vezes uma grandeza para obter outra”, o que depende do contexto em que os conceitos são utilizados; se se tratar de segmentos ou ângulos, por exemplo, teremos de utilizar uma axiomática adequada da Geometria Euclidi-ana, mas podemos pensar no exemplo mais simples dos “sacos de pedras”, escolher determinado saco U de pedras para unidade e será agora fácil compreender o significado de expressões como “o saco B mede p/q unidades U ” ou “ B contém p/q vezes o número de pedras de U ”. Um dos aspectos que torna o exemplo dos sacos de pedra mais elementar que os exemplos geométricos é o facto de dispormos à partida de uma “sub-unidade” – o saco com uma só pedra – que permite sempre, “na pior das hipóteses” obter a “medida” de qualquer saco A tomando para unidade qualquer saco U ; a convicção de que para qualquer tipo de grandeza a situação seria essencialmente a mesma foi abalada cerca de quinhentos anos antes de Cristo devido às descobertas da Escola pitagórica.

Antes de procurarmos compreender o que falha, por exemplo no caso da medida de segmentos, voltemos ainda aos “sacos de pedras”. Notemos que nem sempre é imprescindível recorrer ao saco com uma só pedra; considerando o “saco unidade” U e o “saco a medir” S , podemos começar por tentar separar (dividir...) sucessivamente as pedras de S em grupos, cada um deles em correspondência um-a-um com as pedras de U . Se com este processo esgotarmos exactamente as pedras de S , resta-nos verificar quantos grupos obtivemos³ e é esse número a medida de S tomando U para unidade; se assim não for, podemos subdividir o saco U em certo conjunto de sacos com igual número de pedras⁴, procurando que cada “sub-saco” contenha o maior número possível de pedras⁵. Em seguida usamos um dos “sub-sacos” de U para tentar novamente “medir S ”; na pior das

²Por outras palavras, uma grandeza A “de medida” $1/q$ caracteriza-se pela propriedade de reproduzir a unidade por meio de q “justaposições extremo a extremo”; de uma grandeza B que se pode “preencher exactamente” usando p vezes a grandeza A diz-se que tem medida p/q em termos da unidade inicial.

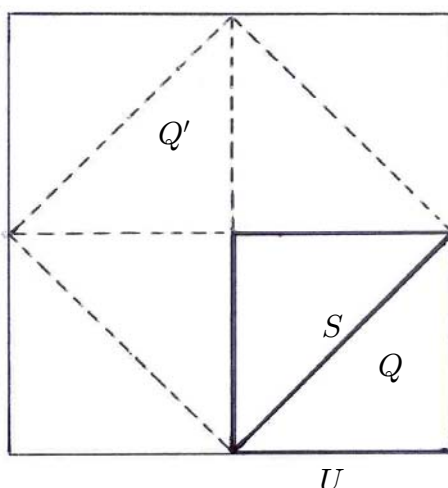
³ou seja, estabelecer uma correspondência um-a-um entre o conjunto dos grupos assim formados e parte da sequência memorizada dos nomes que damos aos números (começando do “um”), pela ordem devida, até esgotarmos esses grupos e atingirmos assim a designação do número de grupos...

⁴Neste momento já é claro o que significa “igual número de pedras”.

⁵Usamos aqui o conceito de “maior número” que também é fácil de relacionar com o estabelecimento de correspondências biunívocas: um conjunto A terá menor número de elementos que B (no sentido lato) se for possível estabelecer uma correspondência um-a-um entre A e uma parte de B .

hipóteses chegaremos ao fim do processo quando cada sub-saco contiver apenas uma pedra, mas é possível que consigamos obter antes a medida de S e em qualquer caso haverá um número mínimo q (na “pior das hipóteses” igual ao número de pedras em U) tal que S pode ser decomposto exactamente em certo número p exacto de sub-sacos cada qual com o mesmo número de pedras que um dos q sub-sacos em que conseguimos decompor U . Diremos então que S “mede” p/q sacos U ou contém p/q vezes o número de pedras de U ; sendo q , por este processo, o menor possível, diremos que a fracção assim obtida é “irredutível”.

Admitamos agora que a mesma possibilidade existe para medir um segmento S utilizando como unidade outro qualquer segmento U (não degenerado), ou seja, admitamos que quaisquer dois segmentos são *comensuráveis*; então tomemos para U o lado de um quadrado Q e para S a respectiva diagonal. A seguinte construção geométrica permite facilmente concluir que um quadrado Q' tendo por lado S se pode decompor em quatro triângulos que reunidos dois a dois permitem “reconstituir” duas vezes o quadrado Q :



Sendo assim, a área de Q' será igual a duas vezes a área de Q . Uma vez que supomos U e S comensuráveis, é possível efectuar a decomposição de U em certo número q de segmentos “iguais a” (ou, mais correctamente, *congruentes*⁶ com) certo segmento V de modo que S se decomponha em p segmentos também congruentes com V . Examinemos então o que se pode concluir quanto às “medidas” dos quadrados Q e Q' ; notemos que a decomposição dos lados de um quadrado em certo número n de partes iguais congruentes com V corresponde a subdivisão do quadrado em pequenos quadrados de lado “igual” a V (um “quadriculado”, como num tabuleiro de xadrez), bastando para tal traçar segmentos paralelos aos lados do quadrado “grande” com extremos nos pontos limites dos sub-segmentos em que se subdividiram os lados. Quantos pequenos quadrados

⁶ É o conceito geométrico resultante da axiomática da geometria que corresponde à ideia intuitiva de segmentos com o mesmo comprimento, ou seja, que, intuitivamente, se podem “sobrepôr exactamente um ao outro”.

assim se obtêm? notemos que os segmentos paralelos a dois dos lados opostos determinam exactamente n rectângulos e os segmentos paralelos aos outros dois lados determinam em cada rectângulo exactamente n quadrados, pelo que teremos no total exactamente $n + \dots + n$ (n vezes) quadrados pequenos, ou seja, abreviadamente, $n \times n$, ou ainda, n^2 quadrados pequenos. Concluimos assim que Q se decompõe em q^2 e Q' em p^2 pequenos quadrados, todos de lados congruentes com V . Neste momento podemos tratar os quadrados “de lado V ” como pedras e os quadrados Q e Q' como sacos de pedras; podemos mesmo imaginar que colocamos uma pedrinha “em cima” de cada quadrado das quadrículas obtidas em Q e Q' . Vejamos o que se deduz da possibilidade de decompor Q' em quatro triângulos que reunidos dois a dois reconstituem Q duas vezes; embora na decomposição em triângulos acima sugerida alguns dos “quadrádivinhos” sejam atravessados pelas diagonais de Q' ficando metade em cada triângulo (e eventualmente um deles dividido em quatro, cada quarto num triângulo distinto), quando reconstituímos Q com dois dos triângulos podemos reconstituir a quadrícula inicial de Q rearrumando os quadrados e as metades e quartos de quadrado que decompõem cada triângulo. Sendo assim, é fácil concluir que a quadrícula de Q' contém exactamente o dobro do número de quadrados da quadrícula de Q ; por outras palavras, em Q' teremos exactamente o dobro das pedrinhas que temos em Q . Esta observação, na aparência inocente, tem consequências dramáticas; com efeito, outro modo de dividir o quadrado Q' em duas metades “iguais” é traçar um segmento de extremos nos pontos médios de dois lados opostos, obtendo-se dois rectângulos, cada um dos quais susceptível de ser “quadrádivinhado” exactamente com metade dos quadrados de Q' ⁽⁷⁾; mas cada um desses rectângulos terá então tantas “pedrinhas” como o quadrado Q , sendo além disso divisível em dois quadrados menores (seja um deles Q''), por um segmento bissectando o lado maior. A situação de Q'' relativamente a Q é agora em tudo idêntica à situação de Q relativamente a Q' : dois quadrados “iguais” a Q'' (constituindo o rectângulo atrás referido) “perfazem a mesma área” que Q , ou seja, o número de pedrinhas que podemos colocar na quadrícula de Q é igual ao dobro do número de pedrinhas da quadrícula de Q'' . Obtivemos uma situação semelhante mas agora com metade das pedrinhas “em jogo”, e podemos recommençar o processo indefinidamente; por outras palavras, se a hipótese inicial fosse viável (“medir a diagonal tomando o lado para unidade”), poderíamos com determinado número inicial de pedrinhas recommençar indefinidamente um processo que conduz em cada passo a “deitar fora” metade das pedrinhas e, com a metade que resta, preencher simultaneamente um quadrado maior e, com o mesmo número de pedrinhas, dois quadrados menores. Em particular o número de pedrinhas que resta em cada passo seria sempre divisível exactamente por dois; mas por maior que fosse o número inicial, ao fim de um número finito de passos chegaríamos fatalmente a apenas uma pedrinha e não poderíamos prosseguir, contradizendo as observações acima feitas – a hipótese inicial não pode assim ser verdadeira. Se quisermos convencer-nos deste

⁷Se o segmento “seccionante” cortasse o interior de uma “fiada” de quadrados da quadrícula, teríamos de cada lado exactamente o mesmo número de metades de quadrados, permitindo reconstituir o mesmo número total de quadrados em cada rectângulo; de facto não seria difícil concluir que esta situação não pode ocorrer neste caso, tendo-se necessariamente o segmento seccionante a passar pelo lado comum de duas “fiadas” contíguas de quadrados, mas não se torna necessário examinar esta questão.

facto sem recorrer à noção de “prosseguir indefinidamente um processo” podemos proceder do seguinte modo: a exemplo do que fizemos com os sacos de pedras, podemos logo começar por escolher q o menor possível⁸; reproduzindo o processo anterior acabamos por concluir que podemos construir dois quadrados de tal maneira que o maior tem lado “igual” à diagonal do menor e em que o menor tem lado $p/2$. Utilizando o teorema de Tales, por exemplo, não seria difícil concluir que, com segmentos proporcionais poderíamos então dividir o lado do quadrado inicial também em $p/2$ segmentos e a respectiva diagonal em q segmentos congruentes com aqueles; ora $p < q + q$ (a diagonal é menor que a soma de dois lados, uma vez que num triângulo qualquer lado é menor que a soma dos outros dois), donde $p/2 < q$, o que contradiz o facto de q ser o *menor* número de partes iguais em que se pode dividir o lado do quadrado para com uma dessas partes “se medir” a diagonal⁹.

A contradição a que se chega por se partir da hipótese de comensurabilidade da diagonal com o lado do mesmo quadrado prova que essa hipótese é insustentável; esta constatação levou os matemáticos gregos posteriores a Pitágoras a privilegiar a Geometria como método de descoberta e progresso em Matemática, relegando a Aritmética e os métodos calculatórios para um papel teórico secundário, ainda que continuasse a ser fundamental nas aplicações. Este “paradigma geométrico” atravessou os milénios até à descoberta do cálculo por Newton e Leibniz no século XVII, sendo notável o facto de na obra magna de Newton (“*Philosophiae Naturalis Principia Mathematica*”) ainda se procurar reduzir sistematicamente todos os argumentos a demonstrações geométricas.

Apesar de tudo, no âmbito da Geometria euclidiana já foram surgindo ao longo dos séculos diversas situações em que se “subvertia” o processo clássico de medição; neste apenas se chegava a um par de números inteiros, ou seja, sendo a medida expressa por uma “*fracção racional*”, eventualmente reduzida a um inteiro (no caso em que o chamado denominador é igual ou pode reduzir-se a 1), pelos métodos atrás descritos, em última análise, o método “dos sacos de pedras”. Noutros casos apenas se podia obter resultados “aproximados” quer se soubesse ou não que o resultado exacto era possível; no caso da medida da diagonal pelo lado do quadrado, por exemplo, sabia-se que a medida exacta era impossível pelo processo clássico mas conseguiam-se obter fracções p/q cujo quadrado se aproximava tanto quanto se quisesse de 2, pelo que cada p/q exprimia a medida de um segmento S' (tomando o lado do quadrado para unidade) de tal modo que a

⁸ Começamos com q igual a um e aumentamos q até “funcionar”; a hipótese de “comensurabilidade” da diagonal com o lado consiste exactamente em supor que “acaba por funcionar” ao fim de certo número q de passos, que será o menor possível por este processo.

⁹Embora tenha sido apresentada de forma “geométrica”, a demonstração de que não existe nenhuma fracção racional cujo quadrado é dois (de onde resulta imediatamente a incomensurabilidade do lado e diagonal do mesmo quadrado, atendendo aos argumentos apresentados), pode basear-se apenas em argumentos “aritméticos”; tomando uma fracção *irredutível* p/q tal que $(p/q)^2 = 2$ virá $p^2 = 2q^2$, pelo que p^2 é par, o que implica que p também o seja, uma vez que o quadrado de um ímpar é também ímpar. Então existe um inteiro k tal que $p = 2k$, pelo que $4k^2 = 2q^2$, donde $q^2 = 2k^2$ e portanto q^2 e q também são pares; mas p e q não podem ser simultaneamente pares, uma vez que se tomou p/q irredutível. Esta contradição prova a inexistência de tal fracção.

diferença entre S' e a diagonal S podia ser tornada tão insignificante quanto se desejasse (no sentido em que podia ser tornada inferior a uma fracção $1/n$ da unidade com n tão grande quanto se quisesse). No famoso caso da medida do perímetro da circunferência tomando o diâmetro para unidade, a própria noção de “medir” uma circunferência, utilizando segmentos que a ela nunca se podem “justapor” exactamente, obrigava a recorrer a processos de aproximação sucessiva; só no século XIX ficou provado que essa medida (designada habitualmente por π) não se podia exprimir por uma fracção racional. Para além dos números inteiros, utilizados nas contagens, e das fracções racionais, também chamadas “números racionais”, invocavam-se entidades algo misteriosas ditas “números irracionais” que desempenhariam o papel de medir... nos casos em que esta operação fosse impossível! No fundo alterava-se o próprio conceito de medição, admitindo-se que, em lugar de se parar num par de inteiros que exprimisse exactamente a referida medida, se poderia em certos casos prosseguir indefinidamente o processo obtendo-se resultados “tão satisfatórios quanto se desejasse” mesmo que nunca fosse possível chegar à medida exacta no sentido clássico. A estes processos generalizados de medida considerava-se estar associado aquilo que se designava por número irracional, mas o uso que deles se fazia (utilizando, nomeadamente, as acima referidas “aproximações”) não estava acompanhado de um conceito tão claramente apreendido como se supunha ser o de número inteiro ou racional.

A introdução dos números negativos é um processo em certa medida paralelo ao acima descrito, mas, apesar de até certo ponto mais tardio, não levanta questões com a complexidade das que atrás ficaram sugeridas. A ideia de generalizar o conceito de número de modo que a subtracção fosse sempre possível encontrava suporte em determinadas utilizações práticas das operações com números, como seja a contabilidade em que o “deve e haver” pode estar desequilibrado para um lado ou para outro tornando-se natural distinguir dois “sentidos” para o valor da diferença consoante o valor mais elevado fosse o “deve” ou o “haver”. Do mesmo modo, grandezas como a temperatura também podiam tomar valores acima e abaixo de determinado ponto “zero” de referência e finalmente a geometria analítica de Descartes sugeria a possibilidade de associar números aos pontos de uma recta, fixando uma origem e um sentido, permitindo assim atribuir “sinais distintos” ao “mesmo” número real quando exprimisse a distância à origem de dois pontos da recta equidistantes desta, cada um “para o seu lado” (curiosamente Descartes nunca aceitou pacificamente os números negativos...). A partir da introdução dos números negativos, passou-se a estender a designação de “número inteiro” também aos números negativos com valor absoluto (módulo) inteiro, pelo que, a menos que não haja perigo de confusão, se deve especificar quando determinado inteiro é positivo ou então designá-lo por “*número natural*”, sinónimo agora de “*inteiro positivo*”.

2. Representação dos números. Sistemas aditivos, multiplicativos e posicionais; exemplos.

Apresentados alguns dos problemas que levaram à consideração de diversos tipos de números, procuremos agora perceber a génese dos processos que levaram

progressivamente às definições rigorosas hoje aceites destes conceitos e dos que lhes são afins. Qualquer dos números atrás referidos (fracções racionais, incluindo os números naturais “começando” em zero, números irracionais, números negativos de qualquer dos tipos anteriores) designa-se por número *real*, pelo que o objectivo final será chegar à definição rigorosa do *conjunto dos números reais* permitindo demonstrar em determinado quadro teórico as respectivas propriedades fundamentais. Antes porém, debruçemo-nos sobre o modo como os diferentes números foram apropriados pelas diversas linguagens humanas.

Já se referiu o processo progressivo que conduziu à elaboração de sequências de expressões orais e escritas em diversas línguas (os nomes dos números, também chamados *numerais*...) cuja memorização permitiu evitar o uso de colecções-padrão constituídas por objectos materiais e substituí-las pelo conjunto destas designações simbólicas. Notemos que o uso do artigo indefinido (um, uma) precede o conceito de número, exprimindo a capacidade que possuímos de individualizar objectos e de os nomear; do mesmo modo temos a noção primitiva de “acrescentar mais um”. Como começámos por notar, certas comunidades não passam quase dessa fase e não têm termos para designar o resultado de mais de um ou dois “acrescentos” à unidade; nas culturas em que se desenvolveu a contagem podem encontrar-se diversos processos sistemáticos para representar os sucessivos números, em princípio sem limite ou com limites “muito elevados”. O uso dos dedos, espalhado por diferentes regiões e épocas, conduziu em muitos casos a sistemas decimais ou vigesimal, por vezes com alguma interferência também dos múltiplos de cinco, de acordo com as características anatómicas humanas (cinco dedos em cada mão e em cada pé, perfazendo dez nas mãos e dez nos pés, portanto vinte no total); em lugar de se inventarem indefinidamente designações e símbolos inteiramente novos à medida que se ia acrescentando uma unidade ao número anteriormente nomeado (o que seria impraticável a partir de certa altura), consideravam-se agrupamentos correspondentes aos dedos de uma ou duas mãos ou das mãos e pés e por diferentes sistemas utilizava-se esses agrupamentos para, de maneira mais ou menos engenhosa, facilitar a memorização das designações e símbolos dos números progressivamente maiores.

Os diferentes sistemas conhecidos podem agrupar-se em dois tipos fundamentais: os *aditivos* e os *multiplicativos*, distinguindo-se no conjunto destes últimos os chamados sistemas “*de posição*”. Todos se baseiam na escolha de uma “*base*” (por vezes misturando duas), ou seja, um número superior à unidade que através das sucessivas potências¹⁰ (começando com a de ordem zero que é igual à própria unidade) permite decompor qualquer número a numa soma em que cada parcela indica quantas vezes a correspondente potência da base “cabe” em a , descontadas as parcelas correspondentes a potências superiores; começando pela maior potência da base imediatamente inferior ao número, esse “número de vezes” associado a cada potência da base pode sempre ser tomado inferior à base, como adiante se concluirá.

¹⁰ Na imagem dos “sacos de pedras”, tomando um saco com um número de pedras igual à base escolhida, podemos constituir os “sacos potência” que são “sacos de sacos”, “sacos de sacos de sacos”, etc. contendo sempre um número de elementos igual à base. Podemos convencionar que o “saco potência de ordem zero” é uma pedra, para que o saco potência de ordem um seja o saco de pedras que inicialmente considerámos...

Nos sistemas aditivos utilizam-se numerais distintos para cada potência da base, o que permite em princípio representar o número sem preocupação de ordenar os numerais representativos do número associado a cada potência da base; como exemplo de sistema aditivo temos a numeração romana, que é até certo ponto “semi-decimal”, uma vez que há símbolos simples para a unidade, cinco, dez, cinquenta, cem, quinhentos, mil e, embora menos usuais, dez mil, etc., a partir dos quais se constroem alguns símbolos compostos de modo a obter-se os grupos de nove símbolos associados a cada potência de dez; além disso a constituição dos símbolos compostos utiliza uma lógica aditiva e em certos casos subtrativa, como veremos. Em cada grupo, o primeiros três símbolos são simples repetições do primeiro (I, II, III, para as unidades, X, XX, XXX, para as dezenas, C, CC, CCC, para as centenas, M, MM, MMM, na forma “moderna”, para os milhares, etc.), o quinto é um novo símbolo, a partir do qual se constrói o quarto, escrevendo à esquerda o primeiro símbolo do grupo, indicando subtração de uma unidade (V e IV, L e XL, D e CD, respectivamente para as unidades, dezenas e centenas) e em seguida o sexto, sétimo e oitavo, acrescentando à direita sucessivamente os três primeiros símbolos do grupo (VI, VII, VIII, para as unidades, LX, LXX, LXXX, para as dezenas e DC, DCC, DCCC para as centenas); finalmente o nono constrói-se a partir do primeiro símbolo do grupo seguinte, acrescentando à esquerda o primeiro símbolo do próprio grupo, indicando subtração de uma unidade (IX, XC, CM, respectivamente para as unidades, dezenas e centenas). Deste modo, por exemplo, o número 1759 representar-se-á por MDCCLIX, sendo usual começar pelo grupo da maior potência de dez e descendo progressivamente, mas seria igualmente compreensível se “baralhássemos” essa ordem (DCCMLIX), ao contrário do nosso sistema de posição que depende estritamente da ordem pela qual escrevemos os algarismos. A numeração romana é particularmente adequada para realizar somas, bastando agregar símbolos e realizar algumas simples substituições (nomeadamente nos símbolos “subtractivos” quando necessário), o que era normalmente feito nos ábacos, mas pouco prática para as outras operações. Por exemplo: M CCC XC VI + DCC L IV = M CCC LXXXX VI + DCC L IIII = M DCCCC LLXXXX VIII = M DDC XXXX VV = MM C XXXXX = MM C L. Esta numeração foi utilizada em contabilidade em certos locais até ao século XVIII.

A numeração grega era também aditiva mas mais estritamente decimal, uma vez que utilizava nove letras do alfabeto grego (acrescentado com três letras arcaicas) para as unidades, outras nove para as dezenas e outras nove para as centenas; para os milhares utilizava as letras das unidades com uma plica do lado esquerdo, no que se aproximava dos sistemas multiplicativos que adiante examinaremos. Para as potências de dez superiores a três utilizava o símbolo M acrescentado superiormente do símbolo correspondente ao número que multiplica 10.000.

Os sistemas multiplicativos utilizam dois tipos de símbolos: numerais representando potências da base e numerais indicando por quanto se deve multiplicar cada potência (a exemplo dos numerais gregos representando milhares e dezenas de milhares); o tradicional sistema de numeração chinês, por exemplo, é multiplicativo. Num sistema multiplicativo podem dispensar-se os numerais representando as diferentes potências da base se se convencionar que os numerais do outro grupo

multiplicam a potência da base correspondente à posição em que são escritos, indicando-se, por exemplo, as potências maiores mais à esquerda e terminando-se sempre na “potência zero” ou seja, na unidade; a única ressalva é que, para evitar ambiguidades, não se pode dispensar a indicação das potências que não apareciam normalmente na notação multiplicativa primitiva, para que a posição de cada numeral indique claramente por qual potência da base se deve multiplicar. Ou seja, será necessário contar com mais um “algarismo” – o que designamos por “zero” – que se coloque nos lugares correspondentes às potências da base que, sendo embora inferiores à maior potência que “cabe” no número dado, eventualmente não sejam utilizadas na construção do número (a omissão das superiores a esta não causa qualquer ambiguidade na notação – trata-se dos “zeros à esquerda”). O sistema de numeração babilónico era deste tipo, de base 60; para a construção dos numerais inferiores a sessenta, que depois eram utilizados na construção dos numerais superiores num sistema de posição, utilizava-se um sistema aditivo de base decimal herdado dos Sumérios e o zero começou por ser indicado por um espaço só mais tarde dando lugar a um símbolo específico. O sistema que hoje utilizamos foi herdado dos Hindús através dos Árabes, como é bem conhecido.

Uma vez de posse de instrumentos linguísticos orais e/ou escritos que nos permitam representar os números inteiros, ficamos aptos, em princípio, a designar também as fracções racionais, utilizando pares de inteiros, mas a ideia de utilizar uma base para os inteiros sugeriu que se adoptassem também designações próprias para as fracções de numerador 1 e denominador igual às potências sucessivas da base e eventualmente para outras fracções mais usuais. Os romanos adoptaram um sistema duodecimal para as fracções, que ainda tem reflexos em alguns sistemas de pesos e medidas ou de moeda, por exemplo nos EUA, ou nas antigas moedas inglesas. Com um sistema de posição, podemos representar qualquer número racional entre zero e um utilizando inversos de potências sucessivas da base; simplesmente, neste caso, não podemos garantir que qualquer fracção inferior a um seja igual a uma soma finita de fracções deste tipo multiplicadas por números inferiores à base. Como veremos, há que recorrer às noções de limite de sucessão e de soma de série; em lugar de uma soma finita podemos ter uma série em que cada parcela é um número inferior à base multiplicado pelo inverso de uma potência da base – o que se chama uma potência de expoente negativo da base. Verifica-se que este tipo de séries quando correspondem a uma fracção racional têm “coeficientes” que a partir de certa ordem reproduzem indefinidamente uma sequência finita de algarismos – trata-se das chamadas “*dízimas*” (utilizando a designação associada à base dez) *finitas* (quando o período se reduz ao algarismo zero) ou “*infinitas periódicas*”. Como é óbvio, com uma simples convenção que permita distinguir onde acaba a “parte inteira” e começa a “parte decimal” de determinada fracção racional, agora não necessariamente inferior a 1, torna-se simples representar num sistema de posição, em determinada base, qualquer número racional, eventualmente afectado do sinal negativo. Nas secções seguintes examinaremos estas questões com mais pormenor.

3. Sistemas posicionais: existência e unicidade da representação de um número natural; algoritmos da soma, subtracção e produto.

O hábito criado de representar os números num sistema de posição quase que nos leva a identificá-los com os conjuntos de símbolos que os representam; para mais a ordenação dos números pode ser facilmente identificada através apenas das respectivas “expansões” em determinada base, em sistema posicional, o que reforça essa ideia. A definição das operações usuais sugere imediatamente também a necessidade de encontrar processos de determinar os algarismos da representação posicional do resultado de uma operação, conhecidos os algarismos representativos dos números sobre os quais ela actua – trata-se dos chamados “*algoritmos*”, palavra com a mesma origem etimológica que “*algarismo*” (nome que se dá aos numerais representativos dos números inferiores à base escolhida), derivando do nome do célebre matemático persa Al-Khowarizmi (séc. IX AD).

A descoberta e justificação dos diversos algoritmos baseia-se no conhecimento que se pode adquirir acerca dos números e das operações e relações que se estabelecem entre eles, utilizando critérios mais ou menos rigorosos de dedução. Levanta-se então a questão de saber em que princípios fundamentar essas justificações; comecemos pela própria representação de um número inteiro em determinada base B (B número inteiro superior a 1). À medida que formos tentando justificar o modo com se processa essa representação utilizaremos propriedades que nos são familiares mas cuja legitimidade terá de ser discutida em fase posterior, incluindo as propriedades básicas das operações sobre números inteiros. Como acima foi referido, qualquer desenvolvimento matemático pressupõe a noção prévia de “unidade” e de “outro” (no fundo, “unidade” e “diversidade”), surgindo desde o início a necessidade de se ter ideia clara do que significa acrescentar “outro” elemento a determinado conjunto de objectos; podemos representar a unidade por 1, como é habitual, conjunto-padrão (“saco de pedras” conceptual) associado a qualquer grupo contendo apenas um objecto e, de cada vez que acrescentamos “outro” objecto a determinado conjunto associado ao “saco de pedras” conceptual n , designamos o novo “saco de pedras” por $n + 1$. Em particular, sendo B superior a 1, será da forma $E + 1$ para certo número natural E superior ou igual a 1. Esta operação e respectivas propriedades podem servir de base às definições sucessivas e propriedades da soma, produto, potência, diferença e quociente de inteiros, bem como da relação de ordem entre inteiros.

Como acima vimos, um sistema posicional exige o uso de um símbolo “zero”; podemos utilizar o símbolo habitual “0”. Pretendemos então justificar a possibilidade de representar qualquer número natural a de maneira única na forma:

$$a = a_0 B^0 + \dots + a_n B^n = \sum_{j=0}^n a_j B^j$$

onde n é determinado número natural e a_0, \dots, a_n são números naturais, $0 \leq a_j < B$, para todo o j de 0 até n , e $a_n \neq 0$; em particular, se for $a = B$ teremos $n = 1$, $a_0 = 0$, $a_1 = 1$.

O sistema posicional, neste caso, consiste em representar o número escrevendo da esquerda para a direita os símbolos representativos dos a_j (algarismos) por

ordem decrescente de índice; o símbolo representativo de a será, neste caso:

$$(a_n \cdots a_0)_B,$$

ou simplesmente

$$a_n \cdots a_0,$$

quando não houver perigo de confusão, onde as reticências substituem os sucessivos símbolos dos números a_j com j estritamente entre n e zero. Em particular o símbolo representativo de B será:

$$10$$

o que não se deve confundir com o número dez, a menos que B seja igual a dez. Analogamente, os símbolos representativos dos sucessivos B^j consistem em escrever 1 à esquerda, seguido de j “zeros”. Podemos assim escrever sempre:

$$a = a_0 10^0 + \cdots + a_n 10^n = \sum_{j=0}^n a_j 10^j = a_0 1 + a_1 10 + \cdots + a_n 10 \dots 0$$

sendo neste caso imprescindível identificar a base do sistema de numeração para que se possa determinar a .

Como justificar a existência e unicidade de tais representações? Seguindo as indicações heurísticas acima apresentadas, devemos começar por procurar n de tal maneira que:

$$B^n \leq a < B^{n+1}.$$

Notemos que n é o maior número natural tal que $B^n \leq a$, ou, de modo equivalente, $n + 1$ é o menor número natural tal que $a < B^{n+1}$; admitamos por agora que é possível encontrar tal número¹¹. Em seguida podemos começar a busca dos a_j ; como atrás foi sugerido, devemos começar pelo maior j (que é n) e procurar determinar “quantas vezes B^n cabe em a ”; esse número de vezes será certo a_n tal que:

$$a_n B^n \leq a, \quad a - a_n B^n < B^n.$$

Analogamente ao que se disse para a determinação de n , a_n fica caracterizado pela propriedade de ser o maior inteiro tal que $a_n B^n \leq a$, ou, em alternativa, por $a_n + 1$ ser o menor inteiro tal que $a < (a_n + 1) B^n$; mais uma vez a existência e unicidade de tais inteiros carece de demonstração, problema cuja análise deixaremos para mais tarde¹². Uma vez que $B^n \leq a$, temos $a_n > 0$, como era requerido. Como encontrar a_n ? Pelo que acabámos de ver, o inteiro a_n é o único

¹¹Uma vez que $B > 1$, notemos que, para qualquer m , $B^{m+1} = B^m B > B^m$; sendo assim, da cadeia de desigualdades $B^m > B^{m-1} > \cdots > B$ relativa a m números, com $B > 1$, deduzimos que $B^m > m$, pelo que bastará tomar $m > a$ para que $B^m > a$. Resta justificar que existe o *menor* m satisfazendo a esta propriedade...

¹²Podemos adiantar que se pode encontrar explicitamente um inteiro m satisfazendo a $a < m B^n$, por exemplo $m = a + 1$, ficando apenas por justificar, tal como acima, a existência do *menor* desses inteiros.

para o qual existe r_n satisfazendo às condições:

$$a = a_n B^n + r_n; r_n < B^n,$$

uma vez que, neste caso, a_n e r_n satisfazem às condições:

$$a_n B^n \leq a < (a_n + 1) B^n; r_n = a - a_n B^n$$

e a existência e unicidade de a_n arrastam evidentemente a de r_n tendo-se, de facto, pelas desigualdades acima:

$$r_n = a - a_n B^n < (a_n + 1) B^n - a_n B^n = B^n.$$

Por outro lado, sendo $a_n + 1$ o *menor* inteiro tal que $a < (a_n + 1) B^n$ e tendo-se também:

$$a < B^{n+1} = B B^n,$$

por definição:

$$a_n + 1 \leq B,$$

e portanto, como era requerido,

$$a_n < B.$$

Encontrámos deste modo o “algarismo de ordem n ” da representação de a na base B e, se $n > 0$, podemos prosseguir, procedendo com r_n de modo análogo ao que fizemos com a . A diferença a assinalar está em que, embora $r_n < B^n$ e poranto só precisemos de utilizar potências de B de expoente inferior a n , nada nos garante que $B^{n-1} \leq r_n$; nada nos impede, no entanto, de procurar a_{n-1} e r_{n-1} tais que:

$$r_n = a_{n-1} B^{n-1} + r_{n-1}; r_{n-1} < B^{n-1}.$$

Analogamente ao que acima fizemos, a_{n-1} será o maior inteiro tal que $a_{n-1} B^{n-1} \leq r_n$ e $r_{n-1} = a - a_n B^n$; simplesmente não podemos garantir agora que $a_{n-1} > 0$, mas continuamos a poder garantir que $a_{n-1} < B$, o que se deduz imediatamente das desigualdades:

$$a_{n-1} B^{n-1} \leq r_n < B^n = B B^{n-1}.$$

Obtivemos já:

$$a = a_n B^n + r_n = a_n B^n + a_{n-1} B^{n-1} + r_{n-1},$$

podendo o processo prosseguir analogamente até se chegar a:

$$a = a_n B^n + r_n = a_n B^n + \dots + a_1 B + r_1,$$

onde $0 < a_n < B$, $a_1, \dots, a_{n-1} < B$, $r_1 < B$. Basta agora pôr $a_0 = r_1$ para se obter todos os algarismos da representação de a na base B .

Para além de propriedades elementares das operações algébricas e da relação de ordem sobre números naturais, utilizámos explícita ou implicitamente algumas propriedades que convém assinalar:

• A existência de “primeiro elemento” ou de “elemento mínimo” para um conjunto de números naturais que tenha pelo menos um elemento (Princípio de boa ordenação).

• A possibilidade de justificar plenamente raciocínios como o acima desenvolvido em que se afirmou a certa altura: “podendo o processo prosseguir analogamente até se chegar a...”. Ou seja, indicou-se como se passava da determinação de a_n, r_n para a determinação de a_{n-1}, r_{n-1} e pressupôs-se que se podia chegar “ao fim” em número finito de “passos análogos”, sem mais justificação; trata-se de um uso implícito do Princípio de indução, de indução matemática ou de indução finita.

Resta ainda provar que a representação acima obtida é única! Começemos por mostrar que n fica determinado de maneira única; basta mostrar que se $m > n$, $a_n, c_m > 0$, e os a_j e c_l são todos inferiores a B então:

$$a_0 B^0 + \cdots + a_n B^n < c_0 B^0 + \cdots + c_n B^n + \cdots + c_m B^m.$$

Se assim for, duas representações do mesmo número na base B nunca poderão ter “ n diferente de m ”, pois nesse caso uma corresponderia a um número *estritamente inferior*, e portanto diferente, da outra. Provemos então a desigualdade; basta verificar que:

$$a_0 B^0 + \cdots + a_n B^n < B^{n+1},$$

uma vez que $n + 1 \leq m$ e portanto:

$$B^{n+1} \leq B^m \leq c_m B^m.$$

Ora, recordando que $B = E + 1$ ($E \geq 1$), e cada $a_j \leq E$, temos:

$$\begin{aligned} a_0 B^0 + \cdots + a_n B^n &\leq E B^0 + \cdots + E B^n = E (B^0 + \cdots + B^n) = \\ &= E (B^0 + \cdots + B^n) + (B^0 + \cdots + B^n) - (B^0 + \cdots + B^n) = \\ &= (E + 1) (B^0 + \cdots + B^n) - (B^0 + \cdots + B^n) = \\ &= B (B^0 + \cdots + B^n) - (B^0 + \cdots + B^n) = \\ &= (B^1 + \cdots + B^{n+1}) - (B^0 + \cdots + B^n) = B^{n+1} - 1 < B^{n+1}, \end{aligned}$$

o que termina a demonstração da unicidade de n .

Seja agora:

$$a = a_0 B^0 + \cdots + a_n B^n = c_0 B^0 + \cdots + c_n B^n,$$

com $a_n, c_n > 0$, e os a_j e c_j todos inferiores a B . Se porventura $n = 0$, teremos imediatamente:

$$a = a_0 = c_0$$

e a demonstração termina. Para $n > 0$ (ou seja, para $n + 1$ parcelas, com $n > 0$), temos:

$$\begin{cases} a = a_0 B^0 + \cdots + a_n B^n = a_0 B^0 + (a_1 B^1 + \cdots + a_n B^n) = \\ \quad = a_0 + B(a_1 B^0 + \cdots + a_n B^{n-1}), \\ a = c_0 B^0 + \cdots + c_n B^n = c_0 + B(c_1 B^0 + \cdots + c_n B^{n-1}), \end{cases}$$

sendo $a_0, c_0 < B$. Ora estas condições garantem que $a_0 = c_0$ e que as somas entre parêntesis são também iguais, uma vez que se trata respectivamente do *resto* e do *quociente* da *divisão inteira* de a por B ; esta unicidade resulta dos mesmos princípios que se utilizaram na determinação sucessiva dos algarismos da representação de a na base B , situação em que se tratou de efectuar divisões inteiras por potências sucessivamente inferiores de B . Temos assim:

$$a_0 = c_0, a_1 B^0 + \cdots + a_n B^{n-1} = c_1 B^0 + \cdots + c_n B^{n-1};$$

ora a última igualdade envolve apenas n parcelas, exactamente nas mesmas condições da hipótese feitas acerca das $n + 1$ parcelas. Quer isto dizer que se tivéssemos já demonstrado o resultado para n parcelas poderíamos agora concluir também que:

$$a_1 = c_1, \dots, a_n = c_n$$

obtendo-se o resultado para $n + 1$ parcelas. Mas, de facto, demonstrámo-lo para 1 parcela ($n = 0$), pelo que resulta deste raciocínio a conclusão para $n = 1$; agora resulta, pela mesma razão, para $n = 1 + 1$, e portanto, sucessivamente, para qualquer n ! Mais uma vez é requerido o *Princípio de Indução* para justificar plenamente a conclusão final da demonstração.

Justificada, com as ressalvas feitas, a representação dos números naturais em qualquer base $B > 1$, poderíamos agora procurar justificar os habituais algoritmos da *soma*, da *multiplicação* e da *subacção*, o que levaria novamente a aplicações do *Princípio de Indução*. Particularmente simples é o algoritmo do produto por potências de B , pois:

$$\begin{aligned} a \times B^k &= (a_0 B^0 + \cdots + a_n B^n) \times B^k = a_0 B^k + \cdots + a_n B^{n+k} = \\ &= 0 B^0 + \cdots + 0 B^{k-1} + a_0 B^k + \cdots + a_n B^{n+k} \end{aligned}$$

e portanto a representação de $a \times B^k$ obtém-se da representação de a acrescentando simplesmente k zeros à direita. Em qualquer caso a aplicação desses algoritmos a operações com outros números obriga a ter acesso a “tabelas” de soma e multiplicação dos números até E (com $E + 1 = B$), ou seja, a conhecer a tabuada... Admitamos que essas justificações estão feitas e pensemos agora no problema da divisão, já acima afluado a propósito da própria representação na base B e da demonstração da unicidade da representação.

4. Divisão inteira; quociente e resto. Algoritmo da divisão; representação posicional das fracções racionais. “Dízimas” finitas, periódicas e infinitas não periódicas; nova abordagem aos números irracionais.

Recordemos que para dois quaisquer números naturais a, b ($b \neq 0$) existem q, r , números naturais únicos tais que:

$$a = qb + r, r < b;$$

q, r caracterizam-se pelas propriedades:

$$qb \leq a < (q+1)b, r = a - qb,$$

ou seja, $q+1$ é o menor inteiro tal que $a < (q+1)b$ (como $b \neq 0$ há inteiros nestas condições, por exemplo $a+1$). Se $a < b$, obviamente $q = 0, r = a$; nos outros casos $q \geq 1$. Como atrás foi referido, q diz-se o *quociente* (inteiro) e r o *resto* da *divisão inteira* de a por b .

Conhecidas as representações de a e b na base B como se obterão as representações de q e r ? Se nos lembrarmos do algoritmo da divisão, na forma como é ensinado em fases elementares da aprendizagem, seremos conduzidos a começar por examinar o caso em que:

$$b \leq a < bB (= 10b);$$

a caracterização de $q+1$ garante que

$$q+1 \leq B$$

e portanto

$$q < B.$$

Neste caso o quociente q exprime-se com um único algarismo, terminando assim a respectiva representação na base B , e os algarismos de r obtêm-se através do algoritmos do produto e da diferença aplicados a $a - qb$. É claro que a determinação de q pode obrigar a algumas tentativas envolvendo já o algoritmo do produto por b e a comparação do resultado com os algarismos da representação de a .

No caso geral podemos notar que, para um expoente k suficientemente grande, teremos:

$$bB^k \leq a < bB^{k+1},$$

o que permite obter pelo processo anterior o quociente q de a por bB^k , dado por um número inferior a B , mas superior a 0. Ter-se-á então:

$$a = qbB^k + r.$$

Como $r < bB^k$ (por definição de divisão inteira), podemos agora dividir $r (= a - qbB^k)$ por bB^{k-1} e, das duas uma, ou $r < bB^{k-1}$ e o quociente é zero sendo o resto r , ou $r \geq bB^{k-1}$ e estamos novamente na situação:

$$bB^{k-1} \leq r < bB^k.$$

Podemos assim prosseguir até chegar a bB^0 , obtendo sempre como quocientes zero ou outro inteiro inferior a B , e como resto final $r < b$. Teremos assim:

$$a = q_k bB^k + \dots + q_0 bB^0 + r = (q_k B^k + \dots + q_0 B^0) b + r,$$

com $q_k > 0, q_0, \dots, q_k < B$, pelo que encontrámos a representação decimal do

quociente q da divisão inteira de a por b , e também a do resto $r = r_0$, que resulta de aplicar os algoritmos do produto e da diferença a $r_1 - q_0 b B^0$.

Para completar a justificação do algoritmo habitual da divisão resta observar que, na determinação do quociente de um número c por $b B^j$ no caso em que:

$$b B^j \leq c < b B^{j+1},$$

não é necessário levar em conta os algarismos da representação de c até à ordem $j - 1$. Com efeito, sendo x o número correspondente a essa parte da representação de c , notemos que $c - x$ se reduz à soma de duas parcelas, da forma:

$$d B^j + e B^{j+1},$$

ou seja,

$$c - x = B^j(d + eB).$$

Então, pondo:

$$d + e B = q b + r_1, \quad r_1 < b,$$

virá (notando que $r_1 \leq b - 1$):

$$c - x = B^j(d + eB) = q b B^j + r_1 B^j, \quad r_1 B^j \leq b B^j - B^j < b B^j,$$

pelo que q será também o quociente da divisão de $c - x$ por $b B^j$. Então, como x é estritamente inferior a B^j (pelo que acima vimos acerca da soma das parcelas correspondentes a uma representação posicional até determinada ordem):

$$c = q b B^j + (r_1 B^j + x), \quad r_1 B^j + x < b B^j - B^j + B^j = b B^j,$$

o que prova que q é também o quociente da divisão de c por $b B^j$; ou seja, este quociente é igual ao da divisão de $d + e B$ por b , o que corresponde a “cortar os algarismos da representação de c até à ordem $j - 1$ ” e dividir por b . Torna-se agora fácil compreender a justeza do algoritmo da divisão, cabendo, no entanto, lembrar que, mais uma vez, seria necessário o *princípio de indução* para justificar cabalmente os raciocínios atrás esboçados.

Vejam os um exemplo; ao dividir 17356 por 41, começamos por dividir 17356 por 4100 ($= 41 \times 10^2$), bastando procurar o quociente de 173 por 41 (pelo processo habitual “tomam-se apenas algarismos suficientes de 17356, começando da esquerda, de modo a obter um número superior ou igual a 41”). Obtemos **4** e o resto seria $17356 - 4 \times 4100 = 17356 - 16400 = 956$, mas, de facto, como vamos dividir agora por 41×10 , poderíamos fazer apenas a divisão de 95 por 41; quer isto dizer que bastaria fazer a diferença entre 1735 e 1640, utilizando apenas mais um algarismo de 17356. É o mesmo que fazer a diferença de 173 e 164 (resto da divisão de 173 por 41) e “baixar o 5”, como se considera habitualmente neste algoritmo; teremos então de obter o quociente de 95 por 41 que é **2**, e agora o resto seria obtido fazendo a diferença $95 - 2 \times 41 = 95 - 82 = 13$ e “baixando” 6 (o mesmo que fazer a diferença entre 956 e 2×410). Finalmente os 136 dividem-se por 41, obtendo-se o quociente **3** e o resto **13**; portanto os algarismos

da representação do quociente na base 10 são 4, 2, 3 e o resto 13, ou seja,

$$17356 = 423 \times 41 + 13.$$

Utilizando fracções racionais podemos agora afirmar que, dados dois inteiros a, b quaisquer, com $b \neq 0$, se $a \geq b$ podemos escrever a/b como soma de um número inteiro com uma fracção em que o numerador é inferior ao denominador; com efeito efectuando a divisão inteira de a por b , obtemos:

$$a = qb + r, \quad r < b,$$

e portanto¹³,

$$\frac{a}{b} = q + \frac{r}{b}, \quad r < b.$$

Qualquer fracção racional (não negativa) pode então ser decomposta na soma de um número natural com uma chamada “*fracção própria*”, em que o numerador é inferior ao denominador; já sabemos representar a chamada *parte inteira* q em sistema posicional com qualquer base, restando agora examinar o modo de representação da chamada “*parte fraccionária*” r/b que, no sistema decimal, também se designa, por abuso de linguagem, a “*parte decimal*”. Se $r = 0$, a parte fraccionária é nula e a/b é igual ao número inteiro q ; supondo $r > 0$ podemos aproveitar o que já sabemos acerca do algoritmo da divisão e notar que para cada k suficientemente grande para que $rB^k \geq b$ podemos obter os algarismos do quociente e do resto da divisão inteira de rB^k por b :

$$rB^k = q_k b + r_k, \quad r_k < b.$$

Como relacionar o sucessivos q_k ? Notemos que multiplicando a equação anterior por B obtemos:

$$rB^{k+1} = q_k B b + r_k B, \quad r_k B < b B$$

e, por outro lado, por definição:

$$rB^{k+1} = q_{k+1} b + r_{k+1}, \quad r_{k+1} < b.$$

Para relacionar q_{k+1} com q_k basta agora efectuar a divisão de $r_k B$ por b :

$$r_k B = q' b + r', \quad r' < b,$$

¹³As regras para operar com fracções podem ser facilmente justificadas informalmente recorrendo ao “modelo dos sacos de pedras”. Por exemplo, $qb/b = q$ significa simplesmente que tomando um saco com b pedras para unidade e “medindo” com ele um saco com qb pedras obtemos q , o que resulta da relação existente entre soma e produto. Analogamente, $(x + y)/b = x/b + y/b$, significa que para “medir” com o mesmo saco de b pedras um saco com $x + y$ pedras podemos medir separadamente dois sacos, um com x pedras e outro com y pedras e adicionar os resultados – trata-se muito simplesmente do pressuposto genérico acerca de operações de medida segundo o qual a medida da reunião de dois conjuntos de entidades sem objectos em comum deverá ser a soma das medidas desses conjuntos. O primeiro resultado pode ser considerado como uma aplicação repetida do segundo para o caso de q parcelas e de modo análogo podemos concluir que $a/b = a'/b'$ sse $ab' = a'b$ e as demais propriedades elementares das operações com números fraccionários.

onde $q' b \leq r_k B < b B$, e portanto $q' < B$. Temos então:

$$rB^{k+1} = q_k B b + q' b + r' = (q_k B + q') b + r', \quad r' < b, \quad q' < B.$$

Pela unicidade do quociente virá então:

$$q_{k+1} = q_k B + q' \quad (q' < B);$$

pelo que acima vimos acerca dos algarismos do produto por B e pelo facto de $q' < B$ sabemos então que a representação posicional de q_{k+1} na base B se obtém da representação de q_k simplesmente acrescentando à direita o algarismo representativo de q' .

Da divisão inteira de $r B^k$ por b podemos agora obter:

$$\frac{r}{b} = q_k \frac{1}{B^k} + \frac{r_k/b}{B^k}, \quad r_k < b;$$

observemos que se k_0 for o menor k tal que $rB^k \geq b$, começando com $k = 1$ os quocientes são todos nulos até se atingir k_0 . Com $k = k_0$, q_k é representado por um único algarismo¹⁴, e, pelo que acabámos de ver, a partir dessa ordem vamos obtendo os sucessivos q_k “acrescentado algarismos à direita”, ou seja, podemos obter sucessivos algarismos $c_1, c_2, \dots, c_{k_0-1}, c_{k_0}, c_{k_0+1}, \dots, c_{k_0+j}, \dots$ tais que:

$$\begin{cases} c_1 = c_2 = \dots = c_{k_0-1} = 0 \\ q_{k_0+j} = c_{k_0+j} B^0 + c_{k_0+j-1} B^1 + \dots + c_{k_0} B^j = (c_{k_0} c_{k_0+1} \dots c_{k_0+j})_B \end{cases}$$

(no caso $k_0 = 1$ não há, evidentemente, “zeros iniciais”). Substituindo na equação anterior, com $k = k_0 + j$ obtemos:

$$\begin{aligned} \frac{r}{b} &= (c_{k_0+j} B^0 + c_{k_0+j-1} B^1 + \dots + c_{k_0} B^j) \frac{1}{B^{k_0+j}} + \frac{r_{k_0+j}/b}{B^{k_0+j}} = \\ &= c_{k_0+j} \frac{1}{B^{k_0+j}} + c_{k_0+j-1} \frac{1}{B^{k_0+j-1}} + \dots + c_{k_0} \frac{1}{B^{k_0}} + \frac{r_{k_0+j}/b}{B^{k_0+j}} = \\ &= c_1 \frac{1}{B^1} + \dots + c_{k_0-1} \frac{1}{B^{k_0-1}} + c_{k_0} \frac{1}{B^{k_0}} + \dots + c_{k_0+j} \frac{1}{B^{k_0+j}} + \frac{r_{k_0+j}/b}{B^{k_0+j}}, \quad r_{k_0+j} < b. \end{aligned}$$

Mas, uma vez que os r_{k_0+j} são todos inferiores a b , ou seja, uma vez que só se dispõe de b valores distintos possíveis para estes restos, antes de se atingir $k = k_0 + b + 1$ terá de se repetir um dos valores anteriores de r_{k_0+j} . Suponhamos que é $r_{k_0+j_0}$ o primeiro valor que se repete, sendo $r_{k_0+j_0+j_1}$ o primeiro “resto” que o iguala; então, pelo modo como se obtêm os sucessivos algarismos “ c ” e os sucessivos “ r ” (divisão inteira por b de cada r multiplicado por B), teremos:

¹⁴Trata-se do primeiro caso que analisámos do algoritmo da divisão.

$$\left\{ \begin{array}{l} c_{k_0+j_0+j_1+1} = c_{k_0+j_0+1}, r_{k_0+j_0+j_1+1} = r_{k_0+j_0+1} \\ c_{k_0+j_0+j_1+2} = c_{k_0+j_0+2}, r_{k_0+j_0+j_1+2} = r_{k_0+j_0+2} \\ \dots \\ c_{k_0+j_0+j_1+j_1-1} = c_{k_0+j_0+j_1-1}, r_{k_0+j_0+j_1+j_1-1} = r_{k_0+j_0+j_1-1} \\ c_{k_0+j_0+2j_1} = c_{k_0+j_0+j_1} = c_{k_0+j_0+1}, r_{k_0+j_0+2j_1} = r_{k_0+j_0+j_1} = r_{k_0+j_0+1}, \\ \dots \end{array} \right.$$

pelo que os algarismos “ c ” e os restos “ r ” se repetem ciclicamente a partir da ordem $k_0 + j_0$ com período j_1 . Pode acontecer que um dos “ r ” seja 0; se assim for, todos os “ c ” e “ r ” seguintes também o serão obviamente, uma vez que o quociente e o resto da divisão inteira de zero por qualquer número são ambos evidentemente iguais a zero; nesse caso chegamos a uma igualdade “sem resto” da forma:

$$\frac{r}{b} = c_1 \frac{1}{B^1} + \dots + c_{k_0-1} \frac{1}{B^{k_0-1}} + c_{k_0} \frac{1}{B^{k_0}} + \dots + c_{k_0+j} \frac{1}{B^{k_0+j}},$$

aquilo que se chama uma “*dízima finita*”, no caso de B ser dez. Para se distinguir a representação desta fracção da representação do número inteiro $(c_1 \dots c_{k_0+j_0})_B$ separa-se a respectiva *parte inteira* (neste caso igual a 0) da representação da *parte fraccionária* por um sinal de pontuação que em certos países é uma vírgula e noutros um ponto; teremos assim, com a notação adoptada em Portugal:

$$\frac{r}{b} = (0, c_1 \dots c_{k_0+j})_B$$

ou, se não houver perigo de confusão:

$$\frac{r}{b} = 0, c_1 \dots c_{k_0+j}.$$

Resta examinar a situação em que nenhum dos r é zero; como vimos, teremos repetição cíclica de uma sequência finita de algarismos e de “restos”. Aliás o caso anterior pode ser considerado como caso particular, em que o ciclo tem período 1 sendo 0 o algarismo “ c ” que se repete indefinidamente; no entanto, nos outros casos, não teremos possibilidade de chegar a uma representação como a anterior apenas com um número finito de algarismos permitindo reconstituir a fracção como soma de produtos desses algarismos com potências sucessivas de $1/B$. Podemos convencionar, por exemplo, que a repetição cíclica indefinida da referida sequência finita de algarismos é indicada colocando essa sequência entre parêntesis, escrevendo, no caso geral e com as notações acima introduzidas (representando $k_0 + j_0$ por n_0):

$$\frac{r}{b} = 0, c_1 \dots c_{n_0-1} (c_{n_0} \dots c_{n_0+j_1-1})$$

(onde, no caso $n_0 = 1$, esta notação significa que não há algarismos antes do parêntesis); por exemplo:

$$\frac{22}{350} = 0,06(285714).$$

Esta notação significará então, exactamente, que, para cada número natural n , se pode escrever:

$$\frac{r}{b} = c_1 \frac{1}{B^1} + \cdots + c_n \frac{1}{B^n} + \frac{r_n/b}{B^n},$$

para certo $r_n < b$, sendo os c_j tais que a partir da ordem n_0 se repete indefinidamente a sequência entre parêntesis, ou seja,

$$c_{n_0+j+mj_1} = c_{n_0+j}$$

para todos os j entre 0 e $j_1 - 1$ e para todos os números naturais m . As somas:

$$c_1 \frac{1}{B^1} + \cdots + c_n \frac{1}{B^n},$$

uma para cada número natural $n \geq 1$, constituem aquilo que se chama uma *sucessão*. Neste caso a sucessão é *crescente*, pois à medida que o n aumenta acrescentam-se parcelas positivas; além disso todas as somas são inferiores a r/b . Ou seja, a sucessão de somas “cada vez mais se aproxima de r/b ” – a diferença entre r/b e a soma correspondente a n decresce à medida que n aumenta; este facto, ao contrário do que por vezes se julga e erradamente se afirma, não garante só por si que possamos encontrar um n suficientemente grande para que a diferença entre r/b e a soma correspondente a n seja inferior a dada fracção positiva, por mais pequena que seja. Ou seja, não garante que entre as somas referidas se possa sempre encontrar uma tão próxima de r/b quanto o desejemos (as seguintes, neste caso, estariam ainda mais próximas); no entanto, neste caso particular, as somas, além de se aproximarem de r/b à medida que n aumenta, tornam-se de facto tão próximas de r/b quanto se quiser (bastando tomar n suficientemente elevado). Com efeito, temos:

$$\frac{r}{b} - c_1 \frac{1}{B^1} + \cdots + c_n \frac{1}{B^n} = \frac{r_n/b}{B^n} < \frac{1}{B^n};$$

se considerarmos um número racional positivo $\delta > 0$, vamos ver que podemos escolher n suficientemente grande para que:

$$\frac{1}{B^n} < \delta.$$

Basta para isso que:

$$B^n > \frac{1}{\delta};$$

ora $1/\delta$ é certa fracção de numerador p , que é um número natural superior ou igual a 1. Teremos encontrado o n requerido se $B^n \geq p$; como $B > 1$, como atrás vimos na nota 11, $B^p > p$, pelo que basta tomar $n \geq p$ para que se tenha a desigualdade requerida e portanto para que:

$$\frac{r}{b} - c_1 \frac{1}{B^1} + \cdots + c_n \frac{1}{B^n} < \delta$$

(sendo a diferença positiva). Exprime-se este facto dizendo que a sucessão das somas *converge* ou *tende para* r/b ou que esta sucessão de somas constitui uma *série convergente com soma* r/b ; note-se que dos r_n apenas utilizámos o facto de se tratar de números naturais inferiores a b . Simbolicamente escrevemos:

$$\frac{r}{b} = \sum_{n=1}^{\infty} c_n \frac{1}{B^n},$$

sendo este o significado preciso que atribuiremos à notação:

$$\frac{r}{b} = 0, c_1 \dots c_{n_0-1} (c_{n_0} \dots c_{n_0+j_1-1}),$$

desde que os c_n tenham a “periodicidade” indicada pela sequência entre parêntesis.

Mostrámos que toda a fracção própria se pode representar como soma de uma série em que a parcela de ordem n é o produto de um número natural c_n inferior a B por $1/B^n$; além disso a sucessão dos c_n tem a propriedade de periodicidade atrás expressa. Dois problemas se nos põem naturalmente:

- 1) *Qualquer sucessão c_1, \dots, c_n, \dots com estas características dará origem a uma série convergente cuja soma é uma fracção racional própria?*
- 2) *Dadas duas sucessões com as referidas características, dando origem ao mesmo número racional, os termos correspondentes serão iguais?*

Dois simples exemplos desenganar-nos-ão acerca da possibilidade de responder positivamente a qualquer destas questões; com efeito, tomemos *todos* os “ c ” iguais a E tal que $E + 1 = B$ ($E = 9$, se a base for dez). Devemos então considerar a sucessão das somas:

$$\begin{aligned} \sum_{j=1}^n E \frac{1}{B^j} &= \sum_{j=1}^n E \frac{1}{(E+1)^j} = \sum_{j=1}^n \frac{E+1}{(E+1)^j} - \sum_{j=1}^n \frac{1}{(E+1)^j} = \\ &= \sum_{j=1}^n \frac{1}{(E+1)^{j-1}} - \sum_{j=1}^n \frac{1}{(E+1)^j} = \\ &= \sum_{j=0}^{n-1} \frac{1}{(E+1)^j} - \sum_{j=1}^n \frac{1}{(E+1)^j} = 1 - \frac{1}{(E+1)^n} = 1 - \frac{1}{B^n}. \end{aligned}$$

Como facilmente agora se conclui, esta sucessão converge para 1, que *não é* uma fracção própria; por outras palavras:

$$1 = 0, (E),$$

ou, na base dez:

$$1 = 0, (9).$$

É agora fácil obter um contra-exemplo para a segunda pergunta; basta tomar $c_1 = 0$ e os restantes iguais a E ; como facilmente se vê, por processo análogo ao acima seguido, virá:

$$\frac{1}{B} = 0,1 = 0,0(E).$$

Ambos os contra-exemplos envolvem uma parte periódica reduzida ao algarismo E (9, se a base for dez); será que excluindo este tipo de partes periódicas só com “Es” já as questões 1) e 2) terão respostas positivas?

Antes de darmos resposta a esta questão convém ainda rever o processo que conduziu à definição dos c_n associados à fracção racional r/b , procurando reconhecer mais algumas propriedades desta sucessão. Notemos que os sucessivos algarismos c_n , a partir do segundo que seja diferente de zero, resultam da divisão inteira de $r_{n-1}B$ por b ; o que significaria obter-se sempre E a partir de certa ordem? teríamos de obter um quociente igual a E para o primeiro resto r_{n-1} igual ao seguinte r_n . Viria então, designando por r' o valor comum a r_{n-1} e r_n :

$$r' B = Eb + r',$$

ou seja:

$$r'(E + 1) = Eb + r',$$

e portanto $r' = b$, uma vez que $E \neq 0$ (já que a base B é maior que 1); mas $r' < b$, uma vez que é o resto de uma divisão por b , pelo que esta situação não pode ocorrer. Ou seja o processo que descrevemos para a obtenção da sucessão dos c_n nunca conduz a uma parte periódica reduzida a “Es” (a nozes, se a base for dez). Vamos então ver que “proibindo” sucessões de algarismos com esta parte periódica, já as respostas às questões 1) e 2) são positivas!

Quanto a 1), tomando a série correspondente à representação:

$$x = 0, c_1 \dots c_{n_0-1} (c_{n_0} \dots c_{n_0+j_1-1})$$

não é difícil concluir que:

$$x = 0, c_1 \dots c_{n_0-1} + \frac{1}{B^{n_0-1}} \times 0, (c_{n_0} \dots c_{n_0+j_1-1});$$

uma vez que (no caso em que $n_0 > 1$):

$$0, c_1 \dots c_{n_0-1} = c_1 \frac{1}{B^1} + \dots + c_{n_0-1} \frac{1}{B^{n_0-1}},$$

tratando-se assim de fracção racional, o mesmo se podendo dizer, evidentemente, de $1/B^{n_0-1}$, basta então demonstrar que $0, (c_{n_0} \dots c_{n_0+j_1-1})$ representa uma fracção própria pois nesse caso a soma das duas parcelas em que decompusemos x será forçosamente uma fracção racional também menor que 1, como é fácil

concluir¹⁵. Para simplificar as notações podemos então examinar o caso de $0, (d_1 \dots d_j)$. Ora,

$$0, (d_1 \dots d_j) = (d_1 B^{j-1} + \dots + d_j B^0) \times \sum_{n=1}^{\infty} \left(\frac{1}{B^j} \right)^n,$$

pelo que ficamos reduzidos a verificar que este produto corresponde de facto a uma fracção própria. Ora a soma da série pode ser facilmente calculada:

$$\begin{aligned} \left(1 - \frac{1}{B^j}\right) \sum_{p=1}^n \left(\frac{1}{B^j}\right)^p &= \sum_{p=1}^n \left(\frac{1}{B^j}\right)^p - \sum_{p=1}^n \left(\frac{1}{B^j}\right)^{p+1} = \\ &= \sum_{p=1}^n \left(\frac{1}{B^j}\right)^p - \sum_{p=2}^{n+1} \left(\frac{1}{B^j}\right)^p = \frac{1}{B^j} - \left(\frac{1}{B^j}\right)^{n+1}, \end{aligned}$$

donde:

$$\sum_{p=1}^n \left(\frac{1}{B^j}\right)^p = \frac{1}{B^j - 1} - \frac{1}{B - 1} \frac{1}{B^{jn}},$$

sucessão de somas que converge, como se vê facilmente, para:

$$\sum_{n=1}^{\infty} \left(\frac{1}{B^j}\right)^n = \frac{1}{B^j - 1}.$$

Mas, como atrás se viu,

$$d_1 B^{j-1} + \dots + d_j B^0 \leq B^j - 1$$

e como, neste caso, os “ d ” não podem ser todos iguais a E (9 se a base for dez), uma vez que excluímos esse tipo de período, teremos mesmo

$$d_1 B^{j-1} + \dots + d_j B^0 < B^j - 1,$$

o que prova que $0, (d_1 \dots d_j)$ representa de facto uma fracção própria, como pretendíamos demonstrar.

Resta provar 2), com a exclusão acima referida, ou seja, resta provar a unicidade da representação posicional das fracções próprias. Supondo que determinada fracção admitia duas representações:

$$0, c_1 \dots c_n \dots = 0, d_1 \dots d_n \dots$$

em que, pelo menos para um j , $c_j \neq d_j$, então, sendo k o menor dos j nestas condições, as séries correspondentes teriam as parcelas todas iguais até à ordem $j - 1$ e seria, por exemplo:

¹⁵Com efeito o produto de $1/B^{n_0-1}$ pela “díxima periódica” é igual ao produto de $1/B^{n_0}$ por um número inferior a B , o que torna x inferior a uma soma finita de produtos de algarismos por potências de $1/B$ de expoente maior que 0, o que já sabemos ser inferior a $1/B^0 = 1$.

$$c_j > d_j$$

(caso contrário trocaríamos os papéis de c e d). Ora é fácil concluir por processos análogos aos acima desenvolvidos que a soma das séries a partir das parcelas $j + 1$ é estritamente inferior a $1/B^j$, pelo que a diferença entre as séries correspondentes aos “ c ” e aos “ d ” terá uma parcela:

$$(c_j - d_j) \frac{1}{B^j} \geq \frac{1}{B^j}$$

e outra em valor absoluto estritamente inferior a $1/B^j$; essa diferença nunca pode ser então igual a zero, contradizendo a igualdade pressuposta.

Fixada uma base $B > 1$, os números racionais não negativos ficam assim “identificados” com as respectivas representações nessa base, da forma:

$$a_k \dots a_0, c_1 \dots c_{n_0-1} (c_{n_0} \dots c_{n_0+j_1-1})$$

podendo ser $n_0 = 0$, caso em que não há algarismos entre a vírgula e o parêntesis, ou $j_1 = 0$, caso em que não existe parte periódica (trata-se nesse caso de uma “dízima finita”, adoptando a designação associada à base dez); além disso podemos sempre supor que o período j_1 é o menor possível, ou seja, que o número de algarismos dentro de parêntesis não pode ser reduzido, e que a parte periódica não se reduz a (E) , onde $E + 1 = B$. Com estas restrições, a representação é única, ou seja, podemos estabelecer uma correspondência biunívoca (um-a-um) entre o conjunto dos racionais não negativos e aquelas representações, ou seja, representações de números naturais na base B seguidas de “ B -díizimas” finitas ou *infinitas periódicas*. Como é evidente, para incluir também os racionais negativos, bastará adoptar um sinal que permita distingui-los dos positivos; no caso de um número negativo utiliza-se habitualmente “ $-$ ” à esquerda da representação do respectivo valor absoluto e com esta convenção ficamos com a possibilidade de indentificar todos os números racionais com aquele tipo de representações, “afectadas ou não de sinal”.

Podemos agora pensar na possibilidade de atribuir significado a “ B -díizimas infinitas não periódicas”. Com efeito, se pensarmos numa sucessão de números naturais inferiores a B ,

$$c_1, \dots, c_n, \dots,$$

com a única restrição de não se tornar identicamente igual a E (como habitualmente, $E + 1 = B$) a partir de certa ordem n , os métodos acima introduzidos permitem estudar a sucessão de somas:

$$c_1 \frac{1}{B^1} + \dots + c_n \frac{1}{B^n}.$$

Os cálculos acima efectuados mostram que para qualquer n , tomando $m > n$ e p qualquer natural, teremos:

$$c_m \frac{1}{B^m} + c_{m+1} \frac{1}{B^{m+1}} + \dots + c_{m+p} \frac{1}{B^{m+p}} < \frac{1}{B^{m-1}} \leq \frac{1}{B^n}.$$

Mas como atrás vimos, para qualquer racional positivo δ , podemos encontrar n suficientemente grande para que $1/B^n < \delta$; deste modo, as somas que acabámos de “estimar” serão todas inferiores a δ ! Por outras palavras, se considerarmos a sucessão inicial de somas até uma ordem suficientemente grande, ou seja, se somarmos parcelas em número suficiente começando da primeira e seguindo pela ordem natural, as que pudéssemos acrescentar daí para a frente só alterariam o valor antes obtido numa quantidade inferior a δ . Diz-se que a sucessão de somas, por este motivo, constitui uma *sucessão de Cauchy*; para efeitos práticos, fixando uma “ordem de aproximação” satisfatória para determinado efeito, podemos sempre encontrar uma soma finita determinada pela “representação B -decimal” associada aos c_n que sirva os nossos propósitos. No entanto sabemos que *não existe* uma fracção racional para a qual convirja a sucessão de somas, a menos que a sucessão dos c_n “se torne periódica a partir de certa ordem”. É fácil encontrar sucessões que não correspondem a “dígitos” finitas nem periódicas; por exemplo a que é sugerida pela sequência:

$$1, 0, 1, 0, 0, 1, 0, 0, 0, 1, \dots$$

com o número de zeros seguidos a aumentar de uma unidade após cada algarismo 1 ⁽¹⁶⁾. Estas sequências ficam associadas às entidades que designamos por números “*irracionais*”; neste caso a “unicidade da representação” pode ser expressa afirmando que se a diferença de duas sucessões de somas associadas a duas representações posicionais infinitas não periódicas convergir para zero, então os algarismos das duas representações são todos respectivamente iguais. A demonstração deste facto pode seguir linhas idênticas às acima apresentadas para o caso das “dígitos” finitas ou infinitas periódicas.

Como exemplo de “*irracional*”, já conhecemos o eventual “número” cujo quadrado fosse igual a 2. Vejamos que é possível encontrar uma “representação posicional” para tal número mesmo sem sabermos muito bem o que “ele é”...

5. Representação posicional de alguns números irracionais; algoritmo da raiz quadrada.

Procuremos então encontrar uma “representação posicional” correspondendo a uma sucessão de números racionais cujo quadrado convirja para 2. Uma vez que “2” não representa nenhum papel particular, vamos substituí-lo por um número natural qualquer p inferior a B^2 (B base do sistema de numeração). Começemos por notar que para cada n natural é possível determinar um número natural y_n satisfazendo à condição:

$$y_n^2 \leq p \times B^{2n} < (y_n + 1)^2;$$

com efeito basta tomar y_n tal que $y_n + 1$ é o menor inteiro positivo cujo quadrado é superior a $p \times B^{2n}$ (ou seja, y_n é o maior inteiro positivo cujo quadrado não ultrapassa $p \times B^{2n}$). Tais inteiros existem (por exemplo, $(p + 1) \times B^n$), pelo que a existência do menor é nova aplicação de um princípio geral (*Princípio de boa*

¹⁶Em particular acabamos de mostrar que *existem sucessões de Cauchy de números racionais que não convergem para um número racional!*

ordenação) cuja análise ainda está por fazer, mas que temos admitido em diversas circunstâncias...

Teremos então:

$$\left(\frac{y_n}{B^n}\right)^2 \leq p < \left(\frac{y_n}{B^n} + \frac{1}{B^n}\right)^2,$$

pelo que:

$$0 \leq p - \left(\frac{y_n}{B^n}\right)^2 < \left(\frac{y_n}{B^n} + \frac{1}{B^n}\right)^2 - \left(\frac{y_n}{B^n}\right)^2 = \left(2\frac{y_n}{B^n} + \frac{1}{B^n}\right)\frac{1}{B^n} \leq (2p + 1)\frac{1}{B^n},$$

de onde facilmente se deduz que a sucessão $(y_n/B^n)^2$ converge para p .

Vamos agora ver que y_n constitui de facto uma sucessão de somas que corresponde a uma “representação posicional na base B ”. Começemos por notar que da hipótese $p < B^2$ se deduz:

$$y_0^2 \leq p \times B^0 = p < B^2$$

e portanto,

$$y_0 < B;$$

y_0 representa-se então por um algarismo x_0 .

Comparemos agora y_{n+1} com y_n ; por definição temos simultaneamente:

$$\begin{cases} y_n^2 \leq p \times B^{2n} < (y_n + 1)^2 \\ y_{n+1}^2 \leq p \times B^{2(n+1)} < (y_{n+1} + 1)^2, \end{cases}$$

donde:

$$\begin{cases} y_n^2 \times B^2 \leq p \times B^{2(n+1)} < (y_n \times B + B)^2 \\ y_{n+1}^2 \leq p \times B^{2(n+1)} < (y_{n+1} + 1)^2, \end{cases}$$

o que obriga a:

$$y_n \times B \leq y_{n+1} < y_{n+1} + 1 < y_n \times B + B,$$

e portanto:

$$y_{n+1} - y_n \times B < B.$$

Concluimos então que y_{n+1} e $y_n \times B$ apenas diferem, quando muito, no algarismo das unidades, que será precisamente igual à diferença entre estes dois valores, no caso de y_{n+1} e zero no caso de $y_n \times B$; por outras palavras, para obter a representação posicional de y_{n+1} na base B a partir da representação de y_n basta “acrescentar à direita desta última representação o algarismo correspondente a $y_{n+1} - y_n \times B$ ”. Partindo do algarismo x_0 que representa y_0 podemos assim obter sucessivamente os algarismos:

$$x_1, \dots, x_n$$

que se vão acrescentando à direita para representar os y_n seguintes; a regra obtida é:

$$x_{n+1} = y_{n+1} - y_n \times B.$$

Como, nesse caso:

$$y_n = x_0 B^n + x_1 B^{n-1} + \dots + x_n B^0,$$

virá:

$$\frac{y_n}{B^n} = x_0 B^0 + \frac{x_1}{B^1} + \dots + \frac{x_n}{B^n}$$

Ou seja, a sucessão y_n/B^n é de facto igual a uma sucessão de somas correspondente a uma “representação posicional na base B ”, com parte fraccionária eventualmente infinita não periódica (como o será certamente, por exemplo, no caso $p = 2$). Nomeadamente, corresponde a:

$$x_0, x_1 \dots x_n \dots$$

Mostremos como podemos obter na prática sucessivamente os algarismos desta representação posicional; como B se representa por 10, passaremos a representar $y_n \times B$ por $10 y_n$ e analogamente para potência superiores de B . Como acima vimos, x_{n+1} obtém-se de y_{n+1} e y_n ; como é y_{n+1} que sabemos caracterizar directamente por uma propriedade de “máximo” (ou “mínimo”, relativamente a $y_{n+1} + 1$), notemos que:

$$y_{n+1} = x_{n+1} + 10 y_n.$$

A caracterização de y_{n+1} envolve o respectivo quadrado, pelo que convém elevar ao quadrado a anterior equação, o que conduz a:

$$\begin{aligned} y_{n+1}^2 &= (x_{n+1} + 10 y_n)^2 = x_{n+1}^2 + 2 \times 10 y_n x_{n+1} + 10^2 y_n^2 = \\ &= x_{n+1}(x_{n+1} + 2 y_n \times 10) + 10^2 y_n^2. \end{aligned}$$

Atendendo a estes cálculos, encontrar o maior y_{n+1} cujo quadrado não ultrapassa $10^{2(n+1)} p$ será o mesmo que encontrar o maior x_{n+1} tal que:

$$x_{n+1}(x_{n+1} + 2 y_n \times 10) \leq 10^{2(n+1)} p - 10^2 y_n^2,$$

ou seja:

$$x_{n+1}(x_{n+1} + 2 y_n \times 10) \leq 10^2 (10^{2n} p - y_n^2)$$

Agora, podemos ainda notar que, pelos cálculos acima aplicados à ordem n :

$$y_n^2 = x_n(x_n + 2 y_{n-1} \times 10) + 10^2 y_{n-1}^2$$

pelo que,

$$10^{2n} p - y_n^2 = 10^2 (10^{2(n-1)} p - y_{n-1}^2) - x_n(x_n + 2 y_{n-1} \times 10).$$

Deste modo o segundo membro da desigualdade pode ser obtido passo a passo; começando com $n = 0$, fazemos a diferença $p - y_0^2$ e multiplicamos por 10^2 (“baixamos dois zeros”). Podemos agora obter o segundo membro da desigualdade no passo $n = 1$, utilizando a última equação; notemos que basta tomar o segundo membro da desigualdade do passo anterior e diminuir-lhe o primeiro membro da mesma desigualdade, multiplicando em seguida por 10^2 , ou seja, “baixando mais dois zeros”. Prosseguindo desta forma, podemos sempre obter o segundo membro da desigualdade utilizando o segundo e primeiro membros da desigualdade na ordem anterior, efectuando a respectiva diferença e “baixando dois zeros” (tal com em situações anteriores, seria necessário o *Princípio de indução* para justificar cabalmente esta conclusão). O primeiro membro da desigualdade obtém-se “dobrando” o valor y_n anteriormente obtido e acrescentando-lhe à direita o novo algarismo x_{n+1} que se pretende “ensaiar” (é o que está indicado dentro do parêntesis), efectuando o produto do número assim obtido pelo próprio x_{n+1} e comparando o resultado com o valor obtido para o segundo membro da desigualdade, até que seja o maior possível mas ainda mantendo a desigualdade. Para terminar, notemos que a “dobragem” de y_n também se pode fazer passo a passo, começando por “dobrar” y_0 e, no passo seguinte, somando simplesmente x_1 a $x_1 + 2y_0 \times 10$, e assim sucessivamente, uma vez que:

$$2y_{n+1} = 2x_{n+1} + 2y_n \times 10 = x_{n+1} + (x_{n+1} + 2y_n \times 10);$$

ou seja, o número $x_{n+1} + 2y_n \times 10$ serve para determinar o próprio x_{n+1} , por produto por este valor e pela avaliação acima descrita, e para preparar o passo seguinte, somando com x_{n+1} para obter o dobro de y_{n+1} e fazendo a diferença do referido produto para o segundo membro da desigualdade para obter o novo segundo membro “baixando dois zeros”.

Não é difícil, com algumas adaptações simples, obter um algoritmo para a raiz quadrada de qualquer número positivo, conhecida a respectiva representação posicional em determinada base. No caso de números inferiores a 10^2 com parte “decimal” não nula, basta em cada passo ir “baixando” dois algarismos da parte decimal, em lugar de “baixar zeros”. Os outros casos podem facilmente reduzir-se a este, começando por dividir por uma potência suficientemente elevada de 10^2 e multiplicando o resultado obtido pela mesma potência de 10 – trata-se de simples “jogo de vírgulas”.

Do mesmo modo, também seria possível deduzir um algoritmo para o cálculo da raiz cúbica, seguindo ideias semelhante e mesmo para raízes de ordem superior, embora, como é óbvio, os cálculos se tornem progressivamente mais laboriosos.

Apresenta-se em seguida um exemplo do cálculo aproximado de $\sqrt{2}$ com uma disposição clássica:

$\sqrt{2,0000000000}$ $\underline{-1}$ 100 $\underline{-96}$ 400 $\underline{-281}$ 11900 $\underline{-11296}$ 60400 $\underline{-56564}$ 383600 $\underline{-282841}$ 10075900 $\underline{8485269}$ 1590631	$1,414213\dots$ $\underline{24}$ $+4$ 281 $\underline{+1}$ 2824 $\underline{+4}$ 28282 $\underline{+2}$ 282841 $\underline{+1}$ 2828423 $\underline{+3}$ 2828426
---	---

Do que precede se conclui que é possível obter uma “representação decimal” correspondente a uma sucessão de racionais cujo quadrado converge para 2, embora a própria representação não corresponda a um número racional. Além disso é fácil concluir que tal representação é a única com esta propriedade de “convergência para 2 do quadrado da sucessão de somas associada”. Gostaríamos de poder identificar essa “representação” exactamente com o número irracional que também designamos por $\sqrt{2}\dots$

6. Fundamentos da Aritmética; a Teoria “ingénua” dos conjuntos. Paradoxos.

Nas secções anteriores acompanhámos alguns desenvolvimentos das ideias que inicialmente conduziram à consideração de diversos tipos de números, acabando por justificar alguns aspectos do sistema de representação numérica que ainda hoje utilizamos. No estabelecimento das regras de utilização desse sistema de representação dos números para efectuar as operações básicas, ou seja, dos chamados *algoritmos* para obter as representações dos resultados dessas operações desde que sejam conhecidas as representações dos “operandos”, utilizámos diversas propriedades dos números inteiros cuja justificação deixámos para fase posterior. Além disso nunca ficou claramente estabelecido o que eram de facto os números dos diversos tipos considerados; recordando os passos que atrás demos, os inteiros naturais identificaram-se com “conjuntos-padrão” que, de colecções de objectos materiais, passaram a colecções de símbolos orais e escritos que permitiam obter os mesmos resultados: registar de modo seguro informação suficiente para se poderem repetir operações de contagem determinadas, ou seja, estabelecimento de correspondências biunívocas.

Pares de inteiros permitem efectuar medidas de carácter mais geral através das regras de utilização das chamadas fracções racionais, e os sistemas de numeração permitem manipular um conjunto limitado de símbolos para representar tanto os inteiros como essas fracções; finalmente em certos casos em que as operações de

medida não podem ser exactamente levadas a cabo apenas com um par de inteiros como resultado final, sabemos enunciar regras que permitem obter sucessivamente resultados em princípio tão próximos do objectivo final quanto o desejemos, sendo cada um desses resultados mais uma vez passível de ser expresso como um par de inteiros. Em certo sentido ficámos dotados de um sistema de representação e de regras aparentemente rigorosas para manipular adequadamente instrumentos conceptuais, que permitem traduzir operações de medida, mas esses instrumentos parecem reduzir-se a convenções de linguagem com uso fundamentado em alguns pressupostos que nos parecem razoáveis, por argumentos que acabam por se reduzir a considerações como as que fizemos com “sacos de pedras”.

A possibilidade de encontrar na Geometria fundamento mais sólido para o uso dos números esbarra evidentemente com o problema da fundamentação da própria Geometria, questão com pergaminhos em certo sentido bem antigos, uma vez que ocupava já muitas mentes na Antiguidade, tendo conduzido à famosa axiomática de Euclides. No entanto foi só em finais do século XIX que se conseguiu expurgar a axiomática de Euclides dos diversos defeitos que lhe foram sendo apontados, cabendo a Hilbert, Tarski, Birkhoff, Pach e outros matemáticos a tarefa de apresentar trabalhos que acabaram por conduzir a uma compreensão e esclarecimento pleno dos fundamentos da Geometria Euclidiana.

Pela mesma época impôs-se o interesse pela fundamentação das propriedades dos números, que eram até aí utilizadas com alguma informalidade; o modo como introduzimos as ideias intuitivas que levaram às noções primitivas de número natural e respectivas operações sugere que, como noção prévia à de número, se pode identificar a noção de “conjunto” ou “coleção de objectos”. Cantor teve a ideia de procurar fundamentar a definição e propriedades básicas dos inteiros naturais numa “Teoria dos Conjuntos” baseada nas relações primitivas de “pertença” e “igualdade”, com propriedades ditadas pelo senso comum; assim, o número de elementos (“cardinal”) de um conjunto A seria muito simplesmente a propriedade comum a todos os conjuntos que se pudessem pôr em *correspondência biunívoca (um-a-um)* com A , a soma de dois números m e n obtinha-se tomando A e B conjuntos sem elementos comuns, A com m elementos, B com n elementos e definindo $m + n$ como o número de elementos do conjunto “união de A com B ”, ou seja do conjunto constituído pelos elementos que “ou estão em A ou em B ”. A própria noção de correspondência biunívoca podia ser fundamentada na Teoria dos Conjuntos através da noção de “par ordenado”; dados a, b , designamos por (a, b) o par ordenado com *primeiro elemento a e segundo elemento b* : uma *correspondência* de um conjunto A para um conjunto B será um conjunto C de pares ordenados tal que o primeiro elemento de cada par de C pertence a A , o segundo a B ; C dir-se-á uma *correspondência unívoca* de A para B (o que também se designa por *função* ou *aplicação* de A em B) se para cada elemento a de A existir um elemento b de B tal que o par ordenado com primeiro elemento a e segundo elemento b está em C , tendo-se além disso:

- Se os pares (a, b) e (a, b') estão em C então $b = b'$.

Designando por *correspondência inversa* de C a correspondência C^{-1} constituída pelos pares (b, a) tais que (a, b) pertence a C , C dir-se-á

correspondência biunívoca entre A e B se C for correspondência unívoca de A para B e C^{-1} correspondência unívoca de B para A . C Também se designa por *bijecção* ou *aplicação bijectiva de A em B* . Não dissemos o que era um par ordenado, mas pretendemos que fique definido sem ambiguidade desde que se indiquem os respectivos elementos a, b e que se indique qual é o *primeiro*; não basta portanto dizer que se trata de um conjunto a que pertencem a, b e mais nenhum elemento (aquilo que se designa por $\{a, b\}$), uma vez que ficaríamos sem indicação de qual o “primeiro” elemento, mas podemos identificar o par ordenado (a, b) com o conjunto $\{a, \{a, b\}\}$, pois este novo conjunto contém toda a informação requerida a um par ordenado. Repare-se que, com esta definição, teremos:

$$(a, b) = (a', b') \text{ se e somente se (sse, abreviadamente) } a = a' \text{ e } b = b',$$

que é exactamente a propriedade requerida aos pares ordenados.

Durante algum tempo admitiu-se que os princípios básicos da Teoria dos Conjuntos eram suficientemente claros e intuitivos para poderem servir de fundamentação a toda a Matemática, com base apenas em manipulações respeitando as regras da Lógica, a qual presidia de qualquer modo a todos os raciocínios considerados correctos. Para além das operações lógicas elementares executadas sobre “relações” (ou seja, *propriedades* ou *proposições* acerca de objectos determinados ou não – constantes ou variáveis), bastaria utilizar a noção de *igualdade* (que se representa habitualmente por $=$) e a de *pertença* (representada em geral por \in) sujeitas a regras ditadas pelo respectivo significado intuitivo. Deste modo “ $x \in A$ ” significaria que “ x é elemento do conjunto A ”, $x = y$ que “ x e y representam o mesmo objecto”, e, em particular, sendo A e B conjuntos, $A = B$ significaria que A e B têm os mesmos elementos, ou, mais formalmente:

Para todo o A, B , $A = B$ sse, para qualquer x , $x \in A$ é equivalente a $x \in B$.

Repare-se que nesta proposição, para além dos símbolos “ \in ” e “ $=$ ” e das letras representando objectos indeterminados (x, A, B) só se usam algumas chamadas “operações lógicas” que permitem construir novas relações a partir de outras dadas; neste caso identificamos “para todo o A, B ” que transforma uma relação contendo as incógnitas (objectos indeterminados) A, B noutra que já não as contém, “sse” (que é outra forma de dizer “é equivalente”), “para qualquer x ”, que transforma uma relação contendo a “incógnita” x noutra que já não a contém e, novamente, ainda que por outras palavras, “é equivalente”. Trata-se portanto de uma relação sem incógnitas, ou seja, aquilo a que se chama uma *proposição*, a qual supomos, neste caso, verdadeira¹⁷; com efeito, repare-se que uma relação com incógnitas pode tornar-se ou não numa proposição verdadeira quando substituímos as incógnitas por objectos determinados, mas outro modo de transformar uma relação com uma incógnita x (seja ela $R(x)$) numa proposição ou numa relação não contendo x como incógnita é utilizar a operação atrás referida que consiste em fazer preceder a relação de “qualquer que seja x ” ou de

¹⁷Pode ser tomada como um dos *Axiomas* da Teoria dos Conjuntos, ditado pelo significado intuitivo das relações e operações lógicas envolvidas. Designa-se habitualmente por *Axioma da Extensão*.

expressão equivalente; simbolicamente costuma representar-se por

$$\forall x, R(x) ,$$

e o significado intuitivo, no caso em que não há incógnitas para além de x , é que substituindo x por qualquer objecto a , $R(a)$ é sempre uma proposição verdadeira. Outro processo de obter uma proposição a partir de $R(x)$ é fazer preceder esta relação de “*Existe x tal que*” ou de uma expressão equivalente, o que se costuma representar por:

$$\exists x : R(x)$$

ou:

$$\exists x, R(x) ;$$

intuitivamente, a nova proposição será verdadeira sse, para pelo menos um a , $R(a)$ o for. As operações que acabámos de descrever e que transformam deste modo relações contendo x em proposições ou em relações já não contendo x designam-se por “*quantificadores*” (respectivamente *universal* – $\forall x$, – e *existencial* – $\exists x :$). Como é evidente, podemos aplicar diversos quantificadores à mesma relação, “quantificando” eventualmente diversas incógnitas, como se fez no acima enunciado *Axioma da Extensão*.

Na definição que acima esboçámos de soma de inteiros podemos reconhecer outra operação lógica; com efeito podemos agora caracterizar o conjunto C que dizemos ter $m + n$ elementos, sabendo que A tem m elementos, que B tem n elementos e que A e B não têm elementos comuns, pela propriedade:

$$x \in C \text{ sse } x \in A \text{ ou } x \in B.$$

A *disjunção* “ou” exprime também uma operação lógica; a própria condição “*A e B não têm elementos comuns*” também se pode escrever:

$$\text{Não existe } x \text{ tal que } x \in A \text{ e } x \in B;$$

mais uma vez só reconhecemos relações envolvendo a noção de “*pertença*” (neste caso particular não se utiliza a “*igualdade*”) e operações lógicas, incluindo, neste caso, para além do quantificador existencial, duas novas operações, expressas respectivamente pelas palavras “*não*” e “*e*”.

Estes exemplos parecem sugerir a ideia de que se podem construir progressivamente todas as noções relativas a números e mesmo toda a Matemática apenas com base nas relações de *pertença* e *igualdade*, conjugadas com as operações lógicas, incluindo os quantificadores. Os “objectos matemáticos” seriam simplesmente conjuntos definidos pelas relações assim construídas; ou seja, dada uma relação $R(x)$, automaticamente teríamos à disposição um “novo” conjunto cujos elementos seriam exactamente os a para os quais $R(a)$ é uma proposição verdadeira. Tal conjunto (“*o conjunto dos x tais que $R(x)$* ”) costuma representar-se por:

$$\{x : R(x)\}$$

As regras da Lógica e um conjunto de princípios derivados do significado intuitivo de “ \in ” e “ $=$ ” permitiriam demonstrar sucessivamente todos os Teoremas básicos a partir dos quais se poderia assim dar um fundamento sólido a toda a Matemática.

Este programa congeminado por Cantor e por outros matemáticos e filósofos como Russel e Whitehead encontrou um obstáculo inesperado numa simples observação de Russel que constitui o “paradoxo” conhecido pelo seu nome. Com efeito, com a noção intuitiva de conjunto, não é habitual ocorrer-nos a possibilidade de um conjunto ser elemento de si próprio: um conjunto de batatas não é uma batata, o conjunto dos números naturais entre dois e cinco não é um número natural entre dois e cinco, etc.; ou seja, os exemplos que mais habitualmente nos ocorrem de conjuntos A satisfazem à relação:

$$A \text{ não pertence a } A,$$

ou, mais “formalmente”, identificando mais claramente a operação lógica e a relação envolvida (mas em pior português...):

$$\text{Não } A \in A,$$

o que se costuma abreviar, escrevendo:

$$A \notin A.$$

Podemos, no entanto, pensar em exemplos de relações que definem conjuntos que são elementos de si próprios; por exemplo o conjunto dos objectos que não são batatas, não é, ele próprio, uma batata, sendo portanto elemento de si próprio. Nada nos parece impedir, em qualquer caso, de reunir todos os conjuntos que não são elementos de si próprios num novo conjunto, ou seja, considerar o conjunto definido pela relação $x \notin x$, que, para mais, exprime uma propriedade que nos parece “habitual” e que só é formada pela aplicação de uma operação lógica (a negação) à relação de pertença. Seja então:

$$C = \{x : x \notin x\};$$

que dizer agora acerca do próprio C ? será que $C \in C$? se fosse o caso, então C não satisfaria à relação $x \notin x$, a qual define C , pelo que $C \notin C$, o que contradiz a hipótese feita. Resta a hipótese de $C \notin C$; mas então, uma vez que C satisfaz à relação $x \notin x$, que define C , forçosamente $C \in C$, o que nos leva também a uma contradição. Ou seja, começámos por provar que necessariamente $C \notin C$ e daí deduzimos que, nesse caso, também $C \in C$, contrariando o princípio básico de não-contradição da Lógica.

O *Paradoxo de Russel* impede-nos de admitir a possibilidade de fundamentar a Teoria dos Conjuntos apenas com os pressupostos intuitivos que no início presidiram à respectiva edificação; em particular seria necessário abandonar a ideia de que qualquer relação construída apenas com as operações e regras da lógica sobre as relações elementares de pertença e igualdade conduziria à definição do conjunto dos elementos que satisfazem a essa relação. Acabamos de apresentar um exemplo de uma tal relação para a qual não podemos admitir a

existência do conjunto dos elementos que a satisfazem¹⁸; seria portanto necessário “regulamentar” cuidadosamente o uso das relações de pertença e igualdade, de modo a evitar paradoxos como este.

Chegados a este ponto, podemos perguntar-nos se o carácter intuitivo e familiar dos números inteiros naturais não sugeriria antes que as respectivas propriedades básicas fossem tomadas como fundamento para o edifício restante da Matemática, abandonando a pretensão de “escavar mais fundo”, fazendo intervir uma “Teoria dos Conjuntos” que afinal se revela menos “sólida” do que previsto. Alguns matemáticos enveredaram por esta via, sendo no entanto de salientar, que, também neste caso, não nos podemos fiar apenas no que nos parecem ser propriedades evidentes; relembremos, por exemplo, a propriedade que utilizámos diversas vezes, segundo a qual qualquer conjunto de números naturais que contenha pelo menos um elemento (conjunto “*não vazio*”) tem elemento mínimo (“*o primeiro elemento*” ou “*o menor elemento*” do conjunto). Este “*Princípio de boa ordenação*”, pode servir de fundamento para o próprio *Princípio de indução* e é, de facto, um dos pilares de toda a Matemática, como ficou sugerido nas secções anteriores. Pensemos então nas diversas designações que podemos construir na língua portuguesa para os números inteiros; só dispomos evidentemente de certo número p de palavras (o número total de palavras “legítimas” da língua portuguesa) pelo que, para designar sem ambiguidade mais do que p números inteiros utilizando apenas palavras portuguesas teremos de recorrer a frases com mais de uma palavra. Sendo assim haverá números que não se podem designar com menos duas palavras e como também só há certo número (inferior ou igual a p^2) de frases portuguesas com exactamente duas palavras, haverá números que necessitam de mais de duas palavras; de modo análogo podemos garantir que há concerteza números que não se podem designar com menos de, por exemplo, dezoito palavras usando uma frase da língua portuguesa; de entre esses, pelo *Princípio de boa ordenação* existirá o menor, ou seja:

O menor número natural que não se pode designar na língua portuguesa com menos de dezoito palavras;

acabámos de o designar exactamente com *dezassete* palavras! Este paradoxo, atribuído a Richard, alerta-nos para os perigos da linguagem informal; considerações como esta levaram alguns matemáticos a procurar “codificar” a linguagem Matemática com base em número limitado de símbolos e em regras cuidadosamente controladas, de modo a evitar os paradoxos e a permitir deduzir, por aplicação rigorosa dessas regras, todos os resultados básicos da Matemática. A chamada escola *Formalista* levou a cabo este programa a partir de finais do século XIX, com base, nomeadamente, nos trabalhos de Hilbert; a pretensão de edificar a Teoria dos Conjuntos e, a partir daí, a ela reduzir toda a Matemática, com base em tal linguagem regulada por um conjunto finito de axiomas, era acompanhada pela proposta de procurar demonstrar a não-contradição da Teoria assim edificada, coroando o edifício com a segurança de que não ocorreriam as situações paradoxais que de início se procuraram evitar. Também se pretendia mostrar que o conjunto escolhido de axiomas era “completo”, no sentido em que qualquer afirmação

¹⁸Diremos que esta relação não é *colectivizante*.

traduzida na referida linguagem formal seria sempre susceptível de ser provada verdadeira ou falsa; ambas as pretensões se viram frustradas pelos trabalhos de Gödel: não é possível demonstrar a não-contradição de qualquer teoria contendo a Aritmética apenas com os princípios da própria teoria, e, por mais axiomas que se acrescentem, é sempre possível encontrar uma nova proposição que não pode ser provada com a axiomática disponível, nem a sua própria negação (diz-se uma proposição *indecidível*). Em 1963 Cohen demonstrou pela primeira vez a “indecidibilidade” de uma conjectura que havia décadas desafiava o engenho dos matemáticos – a chamada “*hipótese do contínuo*”, a que adiante nos referiremos.

De entre as diversas possibilidades que têm sido desenvolvidas para a formalização da Teoria dos Conjuntos vamos abordar resumidamente uma versão ligeiramente modificada da que tem por autoria o matemático fictício Nicolas Bourbaki, pseudónimo de um grupo de conhecidos matemáticos, activos pelo menos desde a primeira metade do século XX; trata-se de uma versão baseada em ideias de Hilbert e de outros matemáticos que precederam a “escola Bourbakista”.

7. Formalização da Teoria dos Conjuntos. Axiomas e operações sobre conjuntos.

Começemos por notar que as diversas operações lógicas, excluindo por agora os quantificadores, ou seja, as que se exprimem pelas palavras “ou”, “e”, “não”, “*implica*” e “*é equivalente a*”, podem, de facto, todas ser expressas através apenas de duas delas, por exemplo “ou” e “não”. Com efeito, analisando o significado que habitualmente se atribui a cada uma destas operações, temos a seguinte tabela de equivalências sucessivas, aplicando-as a duas relações R e S (que podem incluir uma ou mais incógnitas representadas por letras x, y, \dots):

R e S pode ser substituído por não $((\text{não } R) \text{ ou } (\text{não } S))$

R implica S pode ser substituído por $(\text{não } R) \text{ ou } S$

R é equivalente a S pode ser substituído por $(R \text{ implica } S) \text{ e } (S \text{ implica } R)$.

De facto, justifiquemos a primeira: R e S é uma relação que só se torna verdadeira quando ambas as relações R e S o forem; quanto a não $((\text{não } R) \text{ ou } (\text{não } S))$ só será verdadeira quando $(\text{não } R) \text{ ou } (\text{não } S)$ for falsa, ou seja, quando ambas as relações não R , não S forem falsas (uma vez que basta uma delas ser verdadeira para a “*disjunção*” indicada por “ou” ser verdadeira), e portanto quando ambas as relações R e S forem verdadeiras, tal como no caso da “*conjunção*” expressa por “e”.

Quanto à segunda, o significado usual de “*implica*” determina que a relação R implica S pretende garantir que S é verdadeira sempre que R o for, ou seja aquela relação só será falsa se R for verdadeira e S for falsa; do mesmo modo, $(\text{não } R) \text{ ou } S$ só será falsa se não R e S forem ambas falsas, ou seja, se R for verdadeira e S for falsa.

Quanto à terceira, exprime o conceito usual de equivalência como “dupla implicação”.

Deste modo, numa linguagem formalizada em que se procure incluir estas operações lógicas bastará, para esse efeito, tomar para operações primitivas a *negação* e a *disjunção* e considerar as restantes operações como abreviaturas determinadas pelas “substituições” acima expressas. Representemos então a operação “ou” por \vee e a negação por \neg ; para evitar o uso de parêntesis na linguagem formal, em que se pretende fazer economia de símbolos, podemos adoptar a convenção de que os “operandos” a que se aplicam os operadores se escrevem simplesmente por ordem a seguir ao operador que sobre eles actua. Deste modo, se R e S forem relações, podemos representar as relações “ R ou S ” e “não R ”, respectivamente por:

$$\vee RS$$

e

$$\neg R.$$

Com esta convenção podemos por exemplo dizer que “ R e S ”, que muitas vezes se representa por $R \wedge S$, é abreviatura de:

$$\neg \vee \neg R \neg S$$

e que “*implica*”, que se representa também por “ \Rightarrow ”, é simplesmente abreviatura de $\vee \neg$. Seguindo sucessivamente estas regras de substituição, o agrupamento de símbolos que representa “ R é equivalente a S ” (muitas vezes escrito: $R \Leftrightarrow S$) será:

$$\neg \vee \neg \vee \neg RS \neg \vee \neg SR$$

Como se torna claro, o uso sistemático de abreviaturas a que podemos atribuir significado intuitivo, no contexto dos problemas que a Matemática pretende ajudar a resolver, torna-se essencial para possibilitar a apreensão efectiva dos raciocínios que conduzem aos diversos resultados da Matemática; uma vez que as abreviaturas são introduzidas com definições rigorosas utilizando apenas abreviaturas já conhecidas e agrupamentos de símbolos primitivos de acordo com as regras básicas da teoria formalizada, ficamos seguros de que poderíamos sempre recorrer à linguagem formal seguindo as respectivas regras e “desfazendo” passo a passo as abreviaturas. Para determinadas conclusões elementares podemos, no entanto, servir-nos directamente do exame destes agrupamentos de símbolos; por exemplo, no agrupamento que representa $R \wedge S$ podemos identificar o agrupamento $\vee \neg$, que podemos também abreviar em “ \Rightarrow ”. Deste modo, outra maneira possível de exprimir $R \wedge S$ pode ser “não (R implica não S)”, o que talvez não seja óbvio apenas pelo significado intuitivo das operações lógicas, a menos de proceder a uma análise ligeiramente mais extensa.

Relativamente aos quantificadores, notemos que também se pode exprimir um através do outro e da negação; com efeito, o significado que atribuímos a \forall e \exists permite concluir sem dificuldade que, por exemplo, se poderá substituir:

$$\forall x, R(x)$$

por:

$$\text{não } \exists x : \text{não } R(x).$$

Reciprocamente,

$$\exists x : R(x)$$

pode ser substituído por:

$$\text{não } \forall x, \text{não } R(x).$$

Antes de indicarmos como se exprime na linguagem formal um dos quantificadores (o outro pode ser tomado como “abreviatura”, usando uma das regras anteriores), notemos que até agora só sabemos formar relações usando os sinais \in e $=$ e *letras* representando “*incógnitas*”, e compor depois essas relações “primitivas” através das operações lógicas \neg, \vee . Ou seja, a nossa linguagem formal, para já pode incluir *agrupamentos de símbolos* resultantes da junção de \in ou $=$ a um par de letras quaisquer colocadas à respectiva direita, e também os agrupamentos que se obtêm formando com estas relações elementares quaisquer novos agrupamentos sucessivamente resultantes da respectiva junção por aplicação dos símbolos \neg, \vee de acordo com a respectiva regra de utilização (uma só relação á direita de \neg , duas á direita de \vee). Uma sequência de agrupamentos “permitidos” poderá ser:

$$\begin{aligned} &\in xy \\ &= ay \\ &= bd \\ &\vee \in xy = ay \\ &\neg \vee \in xy = ay \\ &\vee \neg \vee \in xy = ay = bd \end{aligned}$$

independentemente do respectivo “significado intuitivo”.

Não temos, por outro lado, nenhum instrumento para construir objectos “concretos” (“conjuntos”, uma vez que nesta formalização da Matemática “objecto” é sinónimo de “conjunto” ou de “termo”); devemos afastar a “tentação” de transformar automaticamente uma relação $R(x)$ num conjunto através da “roupagem”:

$$\{x : R(x)\},$$

pois esta ideia deu “mau” resultado com a relação, aparentemente inócua, $x \notin x$. A solução encontrada para obter objectos cuja manipulação possa conduzir à construção dos diversos conjuntos da Matemática é admitir que os “termos” da teoria, para além das letras (representando intuitivamente incógnitas) possam ser obtidos através de uma nova operação lógica aplicada a relações. Se R contiver a incógnita x , o que se exprime escrevendo “ $R(x)$ ”, fica definido um novo “termo”, “objecto” ou “conjunto” pela expressão:

$$\tau_x R(x) ;$$

τ_x designa-se por *Símbolo de Hilbert* ou *Operação de Hilbert*. A ideia intuitiva é que este objecto satisfaça a própria relação R , ou seja, que, substituindo x por este

“novo objecto”, $R(x)$ se torne numa proposição verdadeira, mas, evidentemente, apenas no caso em que existe pelo menos um objecto satisfazendo a $R(x)$, caso em que a operação de Hilbert serve para fixar um destes objectos de uma vez por todas; caso contrário “nada se diz” acerca deste objecto. Como traduzir formalmente esta ideia intuitiva, uma vez que os próprios quantificadores ainda não estão definidos com rigor, não sendo ainda claro o que se deve exactamente entender, nesta linguagem formal, por “*existe pelo menos um objecto satisfazendo a $R(x)$* ”? A ideia é utilizar precisamente o símbolo de Hilbert para definir o quantificador existencial; assim, por definição, enunciar:

$$\exists x : R(x)$$

será o mesmo que afirmar que o objecto $\tau_x R(x)$ satisfaz à relação $R(x)$; por outras palavras, “ $\exists x : R(x)$ ” é a nova relação que resulta de $R(x)$ substituindo x por $\tau_x R(x)$. Como traduzir estas ideias na construção de agrupamentos de símbolos da nossa linguagem formal? Notemos que o objecto $\tau_x R(x)$ deverá corresponder a um agrupamento de símbolos construído a partir do agrupamento que representamos por $R(x)$, mas de maneira que já não contenha a “incógnita” x , uma vez que agora se trata de um “objecto concreto”, que intuitivamente não deveria depender de substituirmos a incógnita x por outra letra qualquer; a solução encontrada foi introduzir dois novos símbolos destinados à definição desta *operação de Hilbert*. Trata-se do próprio τ e do símbolo \square , para além da possibilidade que se introduz de ligar um τ a um ou mais \square por linhas, cada uma partindo de um τ para um \square ; transforma-se um agrupamento $R(x)$ em $\tau_x R(x)$ simplesmente substituindo cada x de $R(x)$ por um \square , antepondo um τ a todo o agrupamento assim obtido (escrevendo-o à esquerda) e ligando esse τ a cada um dos \square que substituiu cada um dos x . Por exemplo, se $R(x)$ for:

$$\vee \neg = xx \in xx$$

$\tau_x R(x)$ será:

$$\tau \vee \neg = \square \square \in \square \square$$

Nada impede que $R(x)$ contenha outras incógnitas (não é “obrigatório” designar uma relação explicitando sempre todas as incógnitas nela contidas); nesse caso $\tau_x R(x)$ será um objecto ainda “dependente de incógnitas diferentes de x ”, com o qual se podem formar outras relações, às quais se podem aplicar novamente símbolos de Hilbert. Se $R(x, y)$ for $= xy$ e $S(x, y)$ for $\in yx$, podemos, por exemplo, formar sucessivamente os termos:

$$\tau = \square y$$

$$\tau \in y \square$$

e a relação:

$$= \tau = \square y \tau \in y \square$$

seguidos do termo:

$$\tau = \tau = \square \square \tau \in \square \square$$

Temos assim o elenco completo de regras para formar termos e relações na linguagem formal em que pretendemos que seja possível “traduzir” a Matemática. Os agrupamentos de símbolos assim construídos dir-se-ão *termos e relações da Teoria* (neste caso da *Teoria dos Conjuntos* ou da *Matemática*). Para podermos prosseguir, devemos lembrar-nos que o objectivo é obter *Teoremas*, ou seja “*proposições verdadeiras*” deduzidas de acordo com os critérios da Lógica de um conjunto de proposições de partida cuja veracidade se admite (os chamados *Axiomas*) e eventualmente de outros Teoremas que já tenham sido deste modo “*demonstrados*”.

Pretendemos então identificar, de entre os possíveis agrupamentos constituídos de acordo com as regras da linguagem formal, quais os que são *Teoremas*; para começar, de acordo com a interpretação intuitiva que pretendemos dar a esses agrupamentos, deverá tratar-se de *relações* e não de *termos*. Em seguida deveremos começar por estabelecer quais os *Axiomas* que vamos admitir e que constituirão a primeira “lista” de Teoremas, os quais não carecem de mais demonstração que não seja o próprio enunciado; as demonstrações dos restantes Teoremas serão listas de agrupamentos de símbolos da linguagem formal de tal maneira que cada agrupamento da lista é uma relação T para a qual existem anteriormente na referida lista Teoremas S e R (cada um dos quais poderá ser, em particular, um Axioma) tais que R é $S \Rightarrow T$ (em linguagem formal, $\forall \neg ST$). Com esta definição, qualquer agrupamento fazendo parte de uma demonstração será um Teorema.

Para fundamentar a Teoria dos Conjuntos e portanto toda a Matemática, bastará então, em princípio, apresentar a lista dos respectivos *Axiomas*. Cabe aqui esclarecer que, para além dos Axiomas propriamente ditos, que são relações da linguagem formal, podemos admitir os chamados “*esquemas de Axiomas*” que são regras que indicam como construir relações da Teoria; dado um “esquema” e um termo X da Teoria, se $R(x)$ for uma relação construída de acordo com o esquema, $R(X)$ será considerado um Axioma da teoria.

Um primeiro conjunto de axiomas (neste caso construídos com base em esquemas de axiomas) regula o uso das “operações lógicas”, incluindo a operação de Hilbert, e portanto os quantificadores, ou seja, apenas necessita, para a respectiva formulação, para além de letras “representando incógnitas”, dos símbolos $\forall, \neg, \tau, \square$ (com as ligações que se estabelecem entre estes dois últimos símbolos). Com a introdução das abreviaturas habituais das operações lógicas e dos quantificadores e demonstração dos primeiros teoremas, ficamos com um arsenal de métodos de demonstração que traduzem os diversos tipos de raciocínios usuais em teorias hipotético-dedutivas; de aqui em diante utilizaremos sem os explicitar muitos destes resultados, genericamente designados por “regras” ou “leis” da Lógica. O esquema de axiomas que regula o uso dos quantificadores, por exemplo, determina que se a for um termo e $R(x)$ uma relação, $R(a)$ a relação que resulta de $R(x)$ substituindo x por a , então a seguinte relação é um axioma:

$$\bullet R(a) \Rightarrow \exists x : R(x),$$

ou seja, intuitivamente, sempre que for “verdadeira” uma relação da forma $R(a)$ então podemos garantir que é verdadeira a “quantificação” existencial de $R(x)$, ou seja podemos afirmar que “existe x tal que $R(x)$ ”, ou ainda que $R(\tau_x R(x))$.

Em seguida introduzem-se dois esquemas de axiomas envolvendo o símbolo “ $=$ ” e que determinam as propriedades habituais da “igualdade”. O primeiro estabelece que sendo a, b termos, $R(x)$ uma relação, então é um axioma a relação:

$$\bullet (a = b) \Rightarrow (R(a) \Leftrightarrow R(b)),$$

por outras palavras, “se dois termos são iguais podemos indiferentemente substituir a mesma variável por um ou outro em qualquer relação, sem alterar o respectivo valor lógico”; o segundo que, sendo $R(x)$ e $S(x)$ relações, então é um axioma a relação:

$$\bullet (\forall x, R(x) \Leftrightarrow S(x)) \Rightarrow (\tau_x (R(x)) = \tau_x (S(x))),$$

ou seja, são iguais os objectos fixados de uma vez por todas pela operação de Hilbert, associados a relações universalmente equivalentes.

Finalmente introduzem-se os axiomas envolvendo também o símbolo \in , de entre os quais o já acima referido *Axioma da extensão* (cf. nota 16) que estabelece a relação fundamental entre a “igualdade” e a “pertença”; os restantes destinam-se a fixar regras para que determinadas relações “definam conjuntos”, procurando, por um lado, evitar os paradoxos e, por outro, permitir a “construção” de conjuntos suficientes para as necessidades da Matemática. Fixada uma relação $R(x)$, dizemos que $R(x)$ “define um conjunto” ou “é colectivizante em x ” (ou simplesmente “é colectivizante” se não houver perigo de confusão) se for um Teorema a seguinte relação:

$$\exists A : \forall x, (x \in A \Leftrightarrow R(x));$$

neste caso, o objecto, termo ou conjunto:

$$\tau_A (\forall x, (x \in A \Leftrightarrow R(x))),$$

será designado por:

$$\{x : R(x)\}.$$

Este conjunto, além de satisfazer à relação (“em A ”) acima entre parêntesis (escrita depois do símbolo τ_A), por definição do quantificador existencial, é “o único conjunto que satisfaz a essa propriedade”, no sentido em que se B também satisfizer a essa relação, pelo Axioma da extensão e pelas propriedades da “equivalência” (nomeadamente pela *transitividade*) virá:

$$B = \{x : R(x)\}.$$

Além disso, se $R(x)$ for colectivizante em x e $\forall x : (S(x) \Leftrightarrow R(x))$, então $S(x)$ também é colectivizante em x e “define o mesmo conjunto”, ou seja:

$$\{x : R(x)\} = \{x : S(x)\};$$

a segunda parte desta asserção é simples consequência do axioma da extensão e a primeira resulta da definição e propriedades do quantificador existencial e da

transitividade da equivalência (resultante dos axiomas que regulam as “operações lógicas”).

Verifica-se que, para construir os números naturais dentro deste contexto teórico, basta admitir como axiomas que determinadas relações adequadamente escolhidas são *colectivizantes*. Abandonada a esperança de que todas o possam ser, pelo menos partindo de determinado conjunto A e de uma relação $R(x)$ vamos admitir que existe sempre o conjunto dos elementos de A satisfazendo a R , ou seja, que é um axioma a relação:

- A relação “ $x \in A$ e $R(x)$ ” é colectivizante em x ;

acabámos assim de introduzir o esquema de axiomas dito “*Axioma da selecção*”. Note-se que, por este axioma, se para determinada relação $R(x)$ e certo A se tiver:

$$\forall x, (R(x) \Rightarrow x \in A),$$

então $R(x)$ é colectivizante, uma vez que é obviamente equivalente a “ $R(x)$ e $x \in A$ ”.

O Paradoxo de Russel mostra que a relação $x \notin x$ não é colectivizante, mas, se aplicarmos este esquema de axiomas a determinado A e à relação $x \notin x$, o conjunto C que se obtém já não conduz ao paradoxo de Russel, já que, começando por verificar que não se pode ter $C \in C$ (uma vez que, nesse caso, se teria $C \notin C$), concluímos que $C \notin C$, de onde se conclui apenas que também $C \notin A$, uma vez que se $C \in A$ cairíamos na contradição $C \in C$. Utilizando este esquema de axiomas também concluímos que não existe o “conjunto de todos os conjuntos”, ou seja, que a relação $\exists U : (\forall x, x \in U)$ é falsa; com efeito, se assim não fosse, a relação “ $x \notin x$ e $x \in U$ ” seria colectivizante em x , e aplicando o raciocínio anterior ao conjunto C definido por esta relação concluiríamos que $C \notin U$, contra a hipótese feita sobre U . Daqui se conclui que qualquer relação $R(x)$ universal, ou seja, tal que $\forall x, R(x)$ é um Teorema, não pode ser colectivizante.

Apliquemos agora o axioma anterior a A e à relação $x \notin A$; então ficamos a saber que é colectivizante em x a relação “ $x \in A$ e $x \notin A$ ”. Sendo:

$$B = \{x : x \in A \text{ e } x \notin A\},$$

é fácil concluir que $\forall x, x \notin B$, uma vez que se, para determinado a , $a \in B$, ter-se-ia $a \in A$ e $a \notin A$, contradição que, pelas leis da lógica que admitimos já ter demonstrado, prova o que se pretendia. Podemos então concluir que:

$$\exists X : \forall x, x \notin X$$

(estamos a aplicar o esquema de axiomas que regula o quantificador existencial!); por outro lado, se, para determinado C , $\forall x, x \notin C$, é fácil concluir, pelo axioma da extensão, que $C = B$ ⁽¹⁹⁾; em particular, temos:

¹⁹Mostremos que $\forall x, (x \in C \Rightarrow x \in B)$; se assim não fosse, então $\exists x : (x \in C \text{ e } x \notin B)$, contradizendo a hipótese de $\forall x, x \notin C$. Mas trocando os papéis de C e B , concluímos agora que, de facto $\forall x, (x \in C \Leftrightarrow x \in B)$, o que, pelo axioma da extensão, permite imediatamente concluir que $C = B$.

$$B = \tau_C(\forall x, x \notin C),$$

uma vez que o segundo membro da igualdade representa um termo que satisfaz à relação entre parêntesis, por definição do quantificador existencial. Este conjunto é o que se designa por *conjunto vazio* e se representa habitualmente por \emptyset ; ou seja, por definição:

$$\emptyset = \tau_C(\forall x, x \notin C).$$

Pelo axioma da extensão, é fácil agora concluir que qualquer relação *impossível* $R(x)$, ou seja, tal que é um teorema a relação $\forall x, \text{ não } R(x)$, é *colectivizante* e define o conjunto vazio. Por curiosidade, determinemos o agrupamento de símbolos que é \emptyset , na linguagem formal, “desfazendo” sucessivamente as abreviações utilizadas; teremos então a seguinte sequência conduzindo ao agrupamento que é o conjunto vazio da Matemática formalizada:

$$\begin{aligned} & \tau_C(\forall x, x \notin C) \\ & \tau_C(\forall x, \neg \in xC) \\ & \tau_C(\neg \exists x: \neg \neg \in xC) \\ & \tau_C(\neg(\neg \neg \in \tau_x(\neg \neg \in xC)C)) \\ & \tau_C(\neg(\neg \neg \in (\tau \neg \neg \in \square C)C)) \\ & \hline \tau \neg \neg \neg \in \tau \neg \neg \in \square \square \square \end{aligned}$$

Trata-se do primeiro termo “concreto” (sem incógnitas), da Matemática, que definimos e já corresponde a um agrupamento relativamente complexo; a partir daqui nunca será necessário, nem mesmo razoável, escrever deste modo os diversos termos que forem sendo definidos; calcula-se que o número 1, por exemplo, é um agrupamento cuja escrita necessita de dezenas de milhares de símbolos...

Retomemos agora a ideia que preside às operações de contagem, ou seja, “considerar um objecto e acrescentar outro”; então, dados a, b necessitaremos de considerar um conjunto a que pertençam a e b e “mais nenhum objecto”; para isso adopta-se o chamado *Axioma do par*:

- *Quaisquer que sejam a, b , é colectivizante em x a relação: $x = a$ ou $x = b$,*

ou seja, podemos sempre formar o conjunto:

$$\{x : x = a \text{ ou } x = b\},$$

que se representa, em geral, por:

$$\{a, b\}.$$

Agora, dados a, b , podemos começar por considerar $\{a, b\}$ e depois, pelo mesmo axioma, “formar” o conjunto:

$$\{a, \{a, b\}\},$$

que se designa em geral por “*par ordenado de primeiro elemento a e segundo elemento b* ” e se representa por:

$$(a, b),$$

como acima tínhamos referido; ficamos assim habilitados a formar *pares*, “ordenados” ou não, a partir de objectos preexistentes. Notemos que, como caso particular do mesmo princípio, podemos formar os pares $\{a, a\}$ e (a, a) ; quanto ao primeiro, uma vez que são equivalentes as relações “ $x = a$ ou $x = a$ ” e “ $x = a$ ” (pelos axiomas que regulam as operações lógicas e que não explicitámos), teremos, pelo Axioma da extensão:

$$\{a, a\} = \{x : x = a\},$$

conjunto que representaremos, naturalmente, por $\{a\}$, sendo então (a, a) o conjunto $\{a, \{a\}\}$.

Convém agora introduzir a abreviatura \subset , que habitualmente se designa por *inclusão*; $A \subset B$ (que se lê “*A contido em B*” ou “*B contém A*”) representa a relação:

$$\forall x, (x \in A \Rightarrow x \in B).$$

Se $A \subset B$, A diz-se uma *parte de B*; para que seja possível reunir num conjunto as partes de um dado conjunto B introduz-se o chamado *Axioma do conjunto das partes*:

- Qualquer que seja B , é colectivizante em A a relação $A \subset B$.

Designamos por $\mathcal{P}(B)$ o “conjunto das partes de B ”, que este Axioma nos permite formar ou seja:

$$\mathcal{P}(B) = \{X : X \subset B\}.$$

No caso em que $B = \{a\}$, procuremos caracterizar $\mathcal{P}(B)$ através de uma disjunção de igualdades, ou seja, por outras palavras, procuremos “identificar os elementos de $\mathcal{P}(B)$ ”. Começemos por notar que o próprio B satisfaz à condição $B \subset B$, uma vez que, como é de esperar, os axiomas “lógicos” permitem demonstrar que $\forall x, (x \in B \Rightarrow x \in B)$. Seja agora $X \subset B$, $X \neq B$; que objectos poderão pertencer a X ? por definição de $X \subset B$ e de B , teremos sucessivamente (com algum abuso de notação) $\forall x, (x \in X \Rightarrow x \in B \Rightarrow x = a)$, mas para que $X \neq B$, pelo *Axioma da extensão* não poderemos ter também $\forall x, (x = a \Rightarrow x \in X)$, ou seja, ficamos a saber que $a \notin X$; então é fácil concluir que a relação $x \in X$ é impossível e portanto $X = \emptyset$. Temos assim:

$$\forall X : (X \subset B \Leftrightarrow (X = B \text{ ou } X = \emptyset)),$$

pelo que, mais uma vez pelo Axioma da extensão:

$$\mathcal{P}(\{a\}) = \{\emptyset, \{a\}\}.$$

Não é difícil concluir, por raciocínios análogos, que, para qualquer conjunto B , temos sempre $B \subset B$ e $\emptyset \subset B$; em particular, $B \subset \emptyset$ sse $B = \emptyset$, pelo que:

$$\mathcal{P}(\emptyset) = \{\emptyset\},$$

e portanto:

$$\mathcal{P}(\mathcal{P}(\emptyset)) = \mathcal{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}.$$

Os axiomas até agora adoptados permitem-nos já construir inúmeros conjuntos; procuremos agora abordar as operações usuais sobre conjuntos. Como é hábito, designaremos por *intersecção* de dois conjuntos A e B o conjunto:

$$A \cap B = \{x : x \in A \text{ e } x \in B\},$$

sendo de notar que a relação “ $x \in A$ e $x \in B$ ” é obviamente colectivizante, pelo axioma da selecção; podemos mesmo obter a intersecção de “um número arbitrário de conjuntos”, ou seja, geralmente, dado um conjunto \mathcal{A} (“de conjuntos”, o que nesta formalização da Matemática é uma simples redundância...), \mathcal{A} não vazio, definir a intersecção dos conjuntos que pertencem a \mathcal{A} , que será:

$$\bigcap_{C \in \mathcal{A}} C = \{x : \forall C, (C \in \mathcal{A} \Rightarrow x \in C)\}$$

(também se designa, mais simplesmente, por $\bigcap \mathcal{A}$). Notemos, no entanto, que, para garantirmos que é colectivizante em x a relação:

$$\forall C, (C \in \mathcal{A} \Rightarrow x \in C)$$

utilizamos de modo essencial o facto de $\mathcal{A} \neq \emptyset$; neste caso, com efeito, considerando $C_0 \in \mathcal{A}$, a relação $R(x)$ acima que define a intersecção é tal que $\forall x, (R(x) \Rightarrow x \in C_0)$, o que prova que $R(x)$ é colectivizante. No caso em que $\mathcal{A} = \emptyset$, não é difícil concluir que a relação que definiria a intersecção é *universal*, pelo que não pode ser colectivizante, como acima vimos (“definiria o conjunto de todos os conjuntos”).

Pretenderíamos agora definir também a *união* ou *reunião* de A e B através da relação “ $x \in A$ ou $x \in B$ ”, mas os axiomas anteriores não garantem que esta relação seja colectivizante. Também gostaríamos de definir a união “de mais de dois conjuntos”, ou seja, geralmente, dado um conjunto \mathcal{A} , definir o conjunto \mathcal{B} “união dos conjuntos que pertencem a \mathcal{A} ”, que seria:

$$\mathcal{B} = \{x : \exists C : C \in \mathcal{A} \text{ e } x \in C\}$$

(examinando a definição verificamos que \mathcal{B} conteria exactamente os x que estão em pelo menos um C de \mathcal{A} , ou seja, conteria “todos os x dos diversos conjuntos da colecção \mathcal{A} ”). Para tal adopta-se um novo axioma, dito *Axioma da União*:

- Para qualquer \mathcal{A} é colectivizante em x a relação “ $\exists C : C \in \mathcal{A} \text{ e } x \in C$ ” (20);

²⁰Convém generalizar o *Axioma da União*, adoptando um esquema de axiomas que se aplica a “relações $R(x, y)$ dependendo de mais de uma variável”, no seguinte sentido: se para cada y fixado pudermos concluir que os x satisfazendo a $R(x, y)$ pertencem todos a determinado conjunto (o qual pode variar com y), então vamos admitir que para qualquer conjunto Y de ys podemos formar o conjunto:

$$\{x : R(x, y), \text{ para pelo menos um } y \in Y\}.$$

Mais formalmente, estamos a admitir que, dada uma relação $R(x, y)$,

como é óbvio, podemos aplicar este axioma ao conjunto $\mathcal{A} = \{A, B\}$, constituído, pelo axioma do par, a partir de quaisquer A, B , pelo que podemos sempre “formar” a união $A \cup B$.

Outra operação que conduz a conjuntos, como facilmente se vê a partir do axioma da selecção, é a *complementação*; dados C e A , designamos por “*complementar de A em C* ” o conjunto definido pela relação, obviamente colectivizante:

$$x \in C \text{ e } x \notin A;$$

representa-se por:

$$C \setminus A.$$

Em particular, como é óbvio, $C \setminus C = \emptyset$.

Finalmente, mostremos que, dados A, B é possível definir o conjunto dos pares ordenados (a, b) , com $a \in A, b \in B$, ou seja que é colectivizante em x a relação:

$$\exists a : (\exists b : (a \in A \text{ e } b \in B \text{ e } x = (a, b))).$$

Recordemos que, por definição, $(a, b) = \{a, \{a, b\}\}$, tratando-se portanto de um conjunto com um elemento de A e outro que é uma *parte de $A \cup B$* (ou seja, um elemento de $\mathcal{P}(A \cup B)$), e portanto:

$$(a, b) \subset A \cup \mathcal{P}(A \cup B),$$

donde:

$$(a, b) \in \mathcal{P}(A \cup \mathcal{P}(A \cup B)).$$

Deste modo, os x que satisfazem à relação que pretendemos mostrar ser colectivizante, são todos elementos deste último conjunto, construído através dos axiomas (nomeadamente do par, da união e do conjunto das partes); pelo axioma da selecção, tal relação será então colectivizante e define o que se chama o *Produto*

• A relação “para todos os y existe X tal que $\forall x, (R(x, y) \Rightarrow x \in X)$ ”

implica que

para todos os Y é colectivizante em x a relação “ $\exists y : (y \in Y \text{ e } R(x, y))$ ”.

Repare-se que, no caso particular em que $R(x, y)$ é a relação $x \in y$, este esquema implica o axioma da união, uma vez que o antecedente da anterior implicação fica obviamente verificado com $X = y$, e portanto, para todo o Y fica colectivizante a relação “ $\exists y : y \in Y \text{ e } x \in y$ ”, o que é exactamente o axioma da união. Curiosamente, este esquema de axiomas também implica o *esquema de axiomas da selecção*, que pode assim ser dispensado; basta, para isso, considerar, para cada relação $R(x)$, a relação $R(x, y)$ dada por “ $R(x)$ e $x = y$ ” e tomar para X o conjunto $\{y\}$ verificando-se assim o antecedente da implicação, o que mostra que fica satisfeito o consequente, donde, para qualquer Y , é colectivizante em x a relação $\exists y : (y \in Y \text{ e } R(x) \text{ e } x = y)$, ou seja, a relação “ $x \in Y \text{ e } R(x)$ ”, obtendo-se o referido esquema de axiomas da selecção aplicado a $R(x)$. Por estes motivos é usual designar este novo esquema por “*esquema de axiomas da selecção e união*”; a forma mais geral tem importância em algumas questões mais delicadas, por exemplo na teoria dos ordinais.

cartesiano de A por B, que se representa por:

$$A \times B.$$

Seria agora possível demonstrar as diversas propriedades elementares das operações sobre conjuntos.

8. Cardinais; soma e produto. Conjuntos infinitos e números naturais.

Dotados dos instrumentos básicos da Teoria dos conjuntos, podemos agora atacar o problema de definir o *número de elementos de um conjunto A* que também se designa por *Cardinal de A* e se representa muitas vezes por:

$$\# A.$$

Guiados pela experiência que temos da operação de contagem, será natural considerar que *A tem o mesmo número de elementos que B* se existir uma *correspondência biunívoca entre A e B*, noção que definimos na secção 6 e que agora fica perfeitamente identificada com um objecto da nossa Teoria dos Conjuntos formalizada, enquanto parte de $A \times B$, ou seja, conjunto de pares ordenados (a, b) com $a \in A$, $b \in B$, com as propriedades enunciadas na referida secção. Utilizaremos a “abreviatura”

$$A \approx B$$

para a relação “*A tem o mesmo número de elementos que B*” que também se abrevia em “*A é equipotente a B*”. Esta relação tem três propriedades que a caracterizam como “*relação de equivalência*”; nomeadamente é *reflexiva*, ou seja,

$$\forall A, A \approx A,$$

simétrica, ou seja,

$$\forall A, (\forall B, (A \approx B \Rightarrow B \approx A)),$$

e *transitiva*, ou seja,

$$\forall A, (\forall B, (\forall C, ((A \approx B \text{ e } B \approx C) \Rightarrow A \approx C))).$$

As demonstrações fazem-se construindo explicitamente correspondências biunívocas que demonstram as equipotências requeridas; no primeiro caso pode ser a chamada “*identidade*”, correspondência constituída pelos pares (a, a) , com $a \in A$, no segundo e terceiro, admitindo, em cada caso, a existência de correspondências biunívocas que justifiquem os antecedentes das implicações e construindo a partir delas as que justifiquem os consequentes.

Pretendemos então que $\# A$ represente de algum modo a “*propriedade comum*” a todos os conjuntos com o mesmo número de elementos que A (ou seja, equipotentes a A), mas os termos da nossa teoria formalizada não são “*propriedades*”, pelo que deveremos construir $\# A$ pelos processos “*permitidos*”; a solução é, mais uma vez, utilizar o símbolo de Hilbert que, de alguma maneira, fixa um “*padrão*” para contar os elementos de todos os conjuntos equipotentes a A , “*escolhendo um*

deles de uma vez por todas” (existe pelo menos um que é o próprio A , o que significa que a aplicação do símbolo de Hilbert conduz de facto a um conjunto equipotente a A , por definição de quantificador existencial). Teremos então, por definição:

$$\# A = \tau_X(X \approx A),$$

e agora, pelos axiomas que regulam a igualdade, para todo o A, B :

$$A \approx B \Leftrightarrow \# A = \# B.$$

De acordo com o uso que é feito do conceito intuitivo de “zero”, pretendemos que seja o número de elementos do conjunto vazio, ou seja, por definição:

$$0 = \# \emptyset.$$

Como $\emptyset \times A = \emptyset$ (²¹), a existir uma correspondência biunívoca entre \emptyset e A só poderá ser igual a \emptyset ; mas então, nesse caso, necessariamente ter-se-ia $A = \emptyset$, pois se existisse $a \in A$, por definição de correspondência biunívoca teria de existir um par da forma (a, b) na correspondência. Ou seja, o único conjunto equipotente a \emptyset é \emptyset , pelo que, em particular:

$$\# \emptyset = \tau_X(X \approx \emptyset) = \emptyset.$$

De modo análogo, o conceito intuitivo de “unidade” leva-nos a definir:

$$1 = \# \{\emptyset\} = \tau_X(X \approx \{\emptyset\});$$

como atrás ficou referido, não é aconselhável tentar encontrar o agrupamento da nossa linguagem formalizada que ele “de facto é”, uma vez que, como ficou dito, envolve algumas dezenas de milhares de símbolos, sem que o esforço de o escrever seja verdadeiramente gratificante... É fácil concluir que $1 \neq 0$, uma vez que *não se tem* $\{\emptyset\} \approx \emptyset$ (se o fosse, então, pelo que atrás vimos, $\{\emptyset\} = \emptyset$, o que é contradito pelo facto de $\emptyset \in \{\emptyset\}$ e $\emptyset \notin \emptyset$).

Estamos agora aptos a introduzir operações com cardinais, com definições inspiradas nas ideias experimentais que temos acerca das operações com números; procurando formalizar o conceito de soma que já atrás foi abordado, será natural definir a *soma* (ou *adição*) dos cardinais a e b como sendo o *cardinal da união de dois conjuntos disjuntos* A, B (ou seja, com $A \cap B = \emptyset$), tais que $a = \#A$, $b = \#B$. É fácil ver que a soma fica bem definida, ou seja, que não depende da escolha de A e B com as propriedades requeridas, sendo sempre possível encontrar A, B naquelas condições (por exemplo, $A = a \times \{0\}$, $B = b \times \{1\}$); representa-se, como é hábito, por $a + b$, ou seja, em particular:

$$a + b = \#((a \times \{0\}) \cup (b \times \{1\})).$$

Quanto ao produto, pode ser definido através do produto cartesiano; sendo $a = \# A$, $b = \# B$, por definição, o *produto* ou *multiplicação de a por b* será:

²¹Basta notar que se $(a, b) \in \emptyset \times A$, então, por definição, $a \in \emptyset$, o que é absurdo, pelo que $\emptyset \times A$ é de facto também igual a \emptyset .

$$ab = \#(A \times B),$$

o qual também se representa por $a.b$ ou mesmo por $a \times b$, quando não houver perigo de confusão, uma vez que esta última notação também representa o produto *cartesiano* dos conjuntos a e b . Também é fácil concluir que o produto fica assim bem definido (em particular, $ab = \#(a \times b)$) e que valem as propriedades *comutativa* e *associativa* da adição e da multiplicação e a *distributivas* do produto em relação à soma; além disso, 0 é elemento neutro a adição ($a + 0 = 0 + a = a$) e 1 da multiplicação ($a.1 = 1.a = a$). As demonstrações resultam facilmente das correspondentes propriedades das operações acima definidas sobre conjuntos; há que ter cuidado com as chamadas “leis do corte” que valem para números naturais (conceito que ainda não definimos, embora seja óbvio que os números naturais devam ser todos cardinais); com efeito, embora seja verdade que, para todos os cardinais a, b :

$$a + 1 = b + 1 \Rightarrow a = b,$$

já pode acontecer que:

$$a + c = b + c \text{ e } a \neq b.$$

De modo análogo, de $ac = bc$ não podemos concluir que $a = b$, ainda que $c \neq 0$. Para termos ideia de como estas situações são possíveis, admitamos provisoriamente que já “construímos” o conjunto dos números naturais, com as respectivas propriedades habituais e que designamos por \mathbb{N} ; então a aplicação que a n faz corresponder $n + 1$ “transforma” $\mathbb{N} = \{0, 1, \dots, n, \dots\}$ em $\mathbb{N}_1 = \{1, \dots, n, \dots\}$, constituindo uma bijecção (correspondência biunívoca) entre estes dois conjuntos. Então, por definição, $\mathbb{N} \approx \mathbb{N}_1$; designa-se habitualmente por \aleph_0 (pronuncia-se “alefe zero”, uma vez que \aleph é a letra “aleph” do alfabeto hebraico) o cardinal destes conjuntos; uma vez que $\mathbb{N} = \{0\} \cup \mathbb{N}_1$ e $\{0\} \cap \mathbb{N}_1 = \emptyset$, teremos, por definição de soma e de 1:

$$0 + \aleph_0 = \aleph_0 = 1 + \aleph_0,$$

e, no entanto, como acima se viu, $0 \neq 1$!

Notemos, de passagem, que, pelo que acabámos de verificar, \mathbb{N} tem a propriedade “insólita” de ser equipotente a uma sua parte estrita (neste caso, \mathbb{N}_1), ou seja, a um seu sub-conjunto que é dele distinto. Esta propriedade caracterizará \mathbb{N} como *conjunto infinito*; mais precisamente, *definimos* conjunto *finito* com sendo um conjunto A tal que:

- Não existe nenhuma parte estrita X de A tal que $X \approx A$,

ou seja, por outras palavras:

$$\forall X, ((X \subset A \text{ e } X \approx A) \Rightarrow X = A).$$

Um conjunto que não é *finito* dir-se-á *infinito*. O cardinal de um conjunto *finito* dir-se-á também *finito* ou um *número natural*, ou ainda um (*número*) *inteiro positivo*; chegámos assim, finalmente, ao conceito rigoroso de número natural, na formalização que adoptámos da Teoria dos Conjuntos, e portanto da Matemática.

Põe-se a questão de saber se existem *conjuntos infinitos*, e portanto cardinais que não sejam números naturais; aparentemente acabámos de dar um exemplo – o conjunto \mathbb{N} ! – mas temos de reconhecer que não demonstrámos a existência deste conjunto, ou seja, não sabemos se a relação “ x é número natural” é colectivizante em x ... De facto, não se sabe demonstrar esta proposição a partir apenas dos axiomas que introduzimos até agora, pelo que adoptaremos como novo (e último) axioma da Teoria dos Conjuntos exactamente o seguinte (dito “*Axioma do Infinito*”):

- A relação “ x é número natural” é colectivizante em x ;

ou seja, de modo equivalente:

- $\exists C : (x \in C \Leftrightarrow x \text{ é número natural})$.

Podemos agora definir:

$$\mathbb{N} = \{x : x \text{ é número natural}\}$$

e poderíamos demonstrar rigorosamente que \mathbb{N} é *infinito*; reciprocamente, se adoptássemos como axioma a relação “*existe um conjunto infinito*”, poderíamos demonstrar que a relação “ x é número natural” é colectivizante, facto que justifica a designação deste axioma.

É fácil concluir que 0 é número natural, uma vez que \emptyset não contém partes estritas, pelo que nunca poderia ser equipotente a uma delas... Por outro lado se n for número natural, é fácil concluir que $n + 1$ também o é; com efeito, se A tiver n elementos, fixado x tal que $x \notin A$ (x existe sempre, uma vez que A não pode ser o conjunto de todos os conjuntos...), por definição $A \cup \{x\}$ terá $n + 1$ elementos. Ora, se $A \cup \{x\}$ fosse infinito, poderíamos estabelecer uma correspondência biunívoca entre $A \cup \{x\}$ e uma parte estrita B de $A \cup \{x\}$; representemos a correspondência por f e os respectivos pares por $(a, f(a))$ (com $a \in A \cup \{x\}$). Por hipótese, existe $a_0 \in A \cup \{x\}$ tal que $a_0 \notin B$; se $a_0 \neq x$, então $B \setminus \{f(x)\}$ é parte estrita de A , uma vez que não contém a_0 e $a_0 \in A$, pelo que os pares $(a, f(a))$ com $a \in A$ constituem uma correspondência biunívoca entre A e a parte estrita de A que é $B \setminus \{f(x)\}$, o que tornaria A infinito, contra a hipótese. Resta examinar o caso particular em que não podemos escolher $a_0 \neq x$, ou seja, o caso em que $B = A$; mas então os pares $(a, f(a))$ com $a \in A$ constituem uma correspondência biunívoca entre A e $A \setminus \{f(x)\}$, e mais uma vez concluiríamos que A é infinito, contra a hipótese. Portanto, de facto, $A \cup \{x\}$ também é finito, pelo que $n + 1$ é número natural; sendo assim, \mathbb{N} contém 0 e contendo n contém também $n + 1$. Em particular, $1 \in \mathbb{N}$, bem como $2 = 1 + 1$, etc.; reciprocamente é possível demonstrar que *coincide com* \mathbb{N} todo o conjunto $C \subset \mathbb{N}$ tal que $0 \in C$ e se $n \in C$ então $n + 1 \in C$ – trata-se exactamente do *Princípio de Indução* que já temos utilizado informalmente. Com efeito, suponhamos que existia $m \in \mathbb{N}$ tal que $m \notin C$; então, pelo *Princípio de boa ordenação* que também já referimos, existiria o primeiro elemento m nestas condições. $m \neq 0$, uma vez que, por hipótese, $0 \in C$, pelo que $m = n + 1$ para certo $n \in \mathbb{N}$; como m é o menor natural que não está em C e $n < m$, então forçosamente $n \in C$. Mas, nesse caso, por hipótese, $m = n + 1 \in C$, contradição que prova o que desejávamos: $C = \mathbb{N}$. Utilizámos a relação de ordem entre números naturais, o Princípio de boa ordena-

ção e o facto de todo o número natural maior que zero ser da forma $n + 1$ para certo natural n , propriedades e conceitos que não introduzimos com rigor, mas este raciocínio mostra que o *Princípio de indução* resulta facilmente do de *boa ordenação*, mediante a demonstração prévia de alguns resultados simples.

9. Correspondências, funções e famílias; generalização do produto cartesiano, potenciação de conjuntos. Potenciação nos cardinais; operações generalizadas e relação entre soma, produto e potência. Relação de ordem entre cardinais; potências do numerável e do contínuo e hipótese do contínuo. Boa ordenação e princípio de indução em \mathbb{N} .

Dados A, B , tal como a noção de *correpondência biunívoca* entre A e B , também as noções mais gerais de *função* ou *aplicação* de A para B e mesmo a noção geral de *correspondência* entre A e B que introduzimos informalmente na secção 6 podem agora ser formalizadas como partes de $A \times B$. Recordemos a notação habitual para funções; dada uma aplicação f de A para B , costuma representar-se por:

$$f: A \rightarrow B$$

e se $(a, b) \in f$ costuma escrever-se:

$$b = f(a),$$

dizendo-se que b é a *imagem* de a por f . Em determinados casos, dada uma aplicação $x: I \rightarrow B$ representam-se as imagens por x_i em lugar de $x(i)$ e própria aplicação por:

$$(x_i)_{i \in I};$$

no caso particular, por exemplo, em que $I = \{1, 2\}$ (por definição, agora, $2 = 1 + 1$), virá

$$(x_i)_{i \in I} = \{(1, x_1), (2, x_2)\},$$

pelo que, neste caso,

$$(x_i)_{i \in I} = (y_i)_{i \in I}$$

sse

$$x_1 = y_1 \text{ e } x_2 = y_2.$$

Ora esta última condição é característica do par ordenado (x_1, x_2) , pelo que, em certa medida, uma aplicação $(x_i)_{i \in I}$ de I para B , que, com esta notação, também se designa por *família de elementos de B indiciada em I* , acaba por “generalizar” a noção de par ordenado. Ao conjunto-imagem de uma aplicação ($f(A)$, com a notação habitual) também se chama “*conjunto dos elementos da família*”; ou seja, o conjunto dos elementos da família $(x_i)_{i \in I}$ será exactamente:

$$\{x : \exists i \in I : x = x_i\},$$

ou, mais abreviadamente, por abuso de notação:

$$\{x_i : i \in I\}.$$

No caso particular em que $B = B_1 \cup B_2$, o conjunto das famílias $(x_i)_{i \in \{1,2\}}$ tais que $x_1 \in B_1$ e $x_2 \in B_2$ pode “substituir” para “todos os efeitos úteis” o produto cartesiano $B_1 \times B_2$, bastando “identificar” as famílias $(x_i)_{i \in \{1,2\}}$ com os pares ordenados (x_1, x_2) ; esta observação sugere que se generalize a noção de *produto cartesiano* a uma família “de conjuntos” qualquer

$$(B_i)_{i \in I},$$

definindo o *produto cartesiano da família* $(B_i)_{i \in I}$ como sendo o conjunto:

$$\prod_{i \in I} B_i = \{(x_i)_{i \in I} : \forall i \in I, x_i \in B_i\}$$

(adoptando uma notação “abreviada” para a definição do conjunto e para o quantificador, cujo significado agora é óbvio).

Tendo em mente a analogia que acabámos de estabelecer, o conjunto das aplicações de I para A também se designa por “*A levantado a I*” ou “*potência de base A e expoente I*” e representa-se, como era de esperar, por:

$$A^I;$$

com a notação das “famílias” teremos então :

$$A^I = \{(a_i)_{i \in I} : \forall i \in I, a_i \in A\}.$$

Podemos de modo análogo definir os conjuntos *união* e *intersecção* de uma família de conjuntos $(B_i)_{i \in I}$ (supondo $I \neq \emptyset$, para o caso da intersecção), identificando-os respectivamente com a união e intersecção do conjunto dos elementos da família, definidas a secção 7.

Agora é fácil generalizar as operações sobre cardinais; dada uma família de cardinais $(a_i)_{i \in I}$, chamamos *soma* e *produto* da família, respectivamente aos cardinais:

$$\sum_{i \in I} a_i = \# \left(\bigcup_{i \in I} (A_i \times \{i\}) \right)$$

e

$$\prod_{i \in I} a_i = \# \left(\prod_{i \in I} A_i \right)$$

onde, para cada $i \in I$, $a_i = \# A_i$. Não é difícil provar que estas operações estão bem definidas²² e gozam das propriedades comutativa, associativa e distributiva generalizadas; também podemos definir a potenciação, através de:

²²Podemos, além disso, na definição de soma, substituir cada $A_i \times \{i\}$ por qualquer conjunto A'_i desde que A'_i seja equipotente a A_i , para todo o i de I , e $A'_i \cap A'_j = \emptyset$, para todos os $i \neq j$.

$$a^b = \#(A^B),$$

onde $a = \#A$, $b = \#B$, estando igualmente bem definida. Entre as diversas operações existem as relações que se esperam, de acordo com a nossa experiência dos números naturais; com efeito, se para dada família $(a_i)_{i \in I}$ de cardinais existir um cardinal a tal que $\forall i \in I, a_i = a$, então:

$$\sum_{i \in I} a_i = (\#I) \cdot a, \quad \prod_{i \in I} a_i = a^{(\#I)}.$$

Provemos, por exemplo, a segunda; com as notações acima, basta notar que, por definição, no caso em que para cada $i \in I, A_i = A$:

$$\prod_{i \in I} A_i = A^I.$$

Definidas as operações básicas entre cardinais, podemos agora abordar a questão da *ordenação*; como ficou sugerido na secção 1 (nota 5), sendo a, b respectivamente os cardinais de dois conjuntos A, B , é natural dizer que a é *menor ou igual a* b se existir uma *bijecção (correspondência biunívoca) entre A e uma parte de B* . Nesse caso escreveremos:

$$a \leq b$$

e é fácil ver que a relação “ \leq ” entre cardinais fica bem definida deste modo (não depende da escolha de A e B , nas condições requeridas); também se diz que “ b é *maior ou igual a* a ” e escreve-se $b \geq a$. Se $a \leq b$ e $a \neq b$ diremos que a é *menor que* b (ou que b é *maior que* a) e escreveremos:

$$a < b \text{ (ou, respectivamente, } b > a \text{)}.$$

Pelo que vimos na secção anterior, temos, por exemplo, $0 < 1$, e, em geral, é fácil concluir que $a \leq a + b$, para quaisquer cardinais a, b , e $a \leq ab$, se $b \neq 0$; no entanto, como vimos, por exemplo:

$$\aleph_0 = \aleph_0 + 1,$$

e também se demonstra que:

$$\aleph_0 = \aleph_0 + \aleph_0 = \aleph_0 \cdot \aleph_0.$$

Haverá alguma operação que transforme qualquer cardinal num cardinal estritamente superior? Antes de responder a esta questão, comecemos por examinar a relação entre $\#A$ e $\#\mathcal{P}(A)$; é óbvio que a correspondência que a $a \in A$ faz corresponder $\{a\} \in \mathcal{P}(A)$ é uma bijecção de A sobre uma parte de $\mathcal{P}(A)$, pelo que, por definição:

$$\#A \leq \#\mathcal{P}(A).$$

Suponhamos que se tinha:

$$\#A = \#\mathcal{P}(A)$$

e seja $f: A \rightarrow \mathcal{P}(A)$ uma bijecção cuja existência resulta desta igualdade de cardi-

nais; podemos então definir a seguinte parte B de A :

$$B = \{x : x \in A \text{ e } x \notin f(x)\}.$$

Sendo f bijecção, existirá $a \in A$ tal que $B = f(a)$. Será que $a \in B$? suponhamos que sim; então, por definição de B , $a \notin f(a) = B$, contra a hipótese. Concluimos que, certamente, $a \notin B$; então $a \in A$ e $a \notin B = f(a)$, pelo que, por definição de B , $a \in B$, nova contradição que mostra que a hipótese $\#A = \#\mathcal{P}(A)$ é insustentável, uma vez que, em qualquer caso, conduz a uma contradição. Acabámos de provar que:

$$\#A < \#\mathcal{P}(A).$$

Este resultado mostra que podemos sempre construir um cardinal estritamente superior a um dado cardinal; vamos ver que esse novo cardinal pode ser obtido por execução de uma das operações atrás definidas. Com efeito, é fácil concluir que:

$$\#\mathcal{P}(A) = 2^{\#A};$$

basta notar, por exemplo, que $2 = \#\{0, 1\}$, e que, associando a cada parte B de A a aplicação, chamada *função característica de B* , que a cada $a \in A$ faz corresponder 1 se $a \in B$ e 0 no caso contrário, obtemos uma bijecção entre $\mathcal{P}(A)$ e:

$$\{0, 1\}^A,$$

que é exactamente o conjunto das aplicações de A em $\{0, 1\}$. Em resumo, para qualquer cardinal a , tem-se:

$$a < 2^a;$$

em particular, pondo

$$\aleph_1 = 2^{\aleph_0},$$

virá:

$$\aleph_0 < \aleph_1.$$

\aleph_1 diz-se “*Potência do contínuo*”. Durante décadas procurou-se esclarecer a questão seguinte: será que existe um cardinal estritamente situado entre \aleph_0 e \aleph_1 ? A resposta negativa a esta questão é a chamada “*Hipótese do contínuo*”; podemos também definir sucessivamente os cardinais \aleph_n :

$$\aleph_{n+1} = 2^{\aleph_n}$$

obtendo-se uma sucessão de desigualdades:

$$\aleph_0 < \aleph_1 < \dots < \aleph_n < \dots$$

e a *Hipótese do contínuo generalizada* consiste em, para cada n natural, negar a existência de um cardinal x tal que:

$$\aleph_n < x < \aleph_{n+1}.$$

em 1963 Cohen demonstrou que, tanto a Hipótese do contínuo como a generalização que acabámos de enunciar, são *indecidíveis*, podendo ser tomadas como axiomas bem como, em alternativa, as respectivas negações.

Uma consequência importante da desigualdade acima estabelecida é a *inexistência do conjunto de todos os cardinais*; ou seja, a relação “ x é cardinal” não é *colectivizante*. Com efeito, se o fosse, sendo \mathcal{A} o conjunto de todos os cardinais, poderíamos formar a família “identidade em \mathcal{A} ”, constituída por todos os pares (a, a) com a cardinal, seja ela $(x_a)_{a \in \mathcal{A}}$. Seja agora S a soma da família, ou seja:

$$S = \sum_{a \in \mathcal{A}} x_a;$$

teríamos então, para qualquer cardinal b :

$$b \leq b = x_b \leq \sum_{a \in \mathcal{A}} x_a = S < 2^S.$$

Mas, em particular, 2^S é um cardinal, pelo que, pelas desigualdades anteriores, com $b = 2^S$,

$$2^S < 2^S,$$

absurdo que demonstra a inexistência do conjunto \mathcal{A} .

Facilmente se verifica que a relação \leq entre cardinais é *reflexiva*, ou seja:

$$a \leq a,$$

para todo o cardinal a e *transitiva*, ou seja, para todos os cardinais a, b, c :

$$(a \leq b \text{ e } b \leq c) \Rightarrow a \leq c.$$

Para demonstrar que é uma *relação de ordem parcial (lata)* faltaria provar que é *antisimétrica lata*, ou seja, para quaisquer cardinais a, b :

$$(a \leq b \text{ e } b \leq a) \Rightarrow a = b,$$

e para provar que se trata de *relação de ordem total (lata)* faltaria depois demonstrar que para quaisquer cardinais a, b se tem:

$$a \leq b \text{ ou } b \leq a.$$

Estas duas últimas propriedades são também verdadeiras, mas de demonstração bastante mais delicada, devida a Schröder e Bernstein; a demonstração pode basear-se na análise da questão da “*boa ordenação*” que já foi abordada a propósito das propriedades dos números naturais. Um par ordenado constituído por um conjunto X e uma correspondência C de X para X de tal maneira que a relação “ $x \leq y$ ” definida por $(x, y) \in C$ é de ordem total lata diz-se um “*Conjunto totalmente ordenado*” (a relação “ $x \leq y$ e $x \neq y$ ” representa-se habitualmente por $x < y$) e C diz-se uma *ordem total* sobre X . Um conjunto totalmente ordenado (X, C) diz-se *bem ordenado* se qualquer parte não vazia Y de X tiver “primeiro elemento”, ou seja se existir $y_0 \in Y$ tal que $y_0 \leq y, \forall y \in Y$; o primeiro

elemento de Y , se existir, é único, como facilmente se verifica. A ordem total de um conjunto bem ordenado diz-se uma *boa ordem*.

Demonstra-se que todo o conjunto *pode ser bem ordenado*; ou seja, que dado X existe sempre uma boa ordem sobre X . O estudo deste conceito pode levar à demonstração do *Teorema de Schröder-Bernstein* e também à demonstração de que, em qualquer conjunto de cardinais, a relação \leq acima considerada define uma *boa ordem*. Em particular “ \mathbb{N} é bem ordenado”; pelo que se viu no final da secção anterior fica então também provado o *Princípio de indução*. Com estes princípios ficaríamos habilitados a demonstrar rigorosamente, sem dificuldade, todos os teoremas básicos da Aritmética; em particular, fixada uma base B (qualquer número natural maior que 1), podemos estabelecer uma correspondência biunívoca entre \mathbb{N} e o conjunto das sequências finitas (a_0, \dots, a_k) de números naturais, com $k \geq 0$, $a_k > 0$, $a_0, \dots, a_k < B$, acrescentado com a sequência (0), que a cada número natural n faz corresponder a sequência dos algarismos da respectiva representação na base B . Definindo a soma e o produto de sequências daquele tipo através dos algoritmos da soma e produto referidos na secção 3, poderíamos verificar que aquela correspondência biunívoca é um isomorfismo de grupóides (cf. a secção seguinte) para as operações de adição e multiplicação. Também poderíamos caracterizar a ordem em \mathbb{N} através das representações em determinada base; como é fácil concluir, se:

$$a = (a_k \dots a_0)_B, b = (b_l \dots b_0)_B$$

então $a < b$ sse $a \neq b$ (ou seja, se $k \neq l$ ou $k = l$ mas existir j tal que $a_j \neq b_j$) e:

$$k < l \text{ ou } (k = l \text{ e } a_{j_0} < b_{j_0}, \text{ sendo } j_0 \text{ o maior } j \text{ tal que } a_j \neq b_j).$$

10. Subtração em \mathbb{N} . O anel \mathbb{Z} dos números inteiros relativos.

A *adição e multiplicação* em \mathbb{N} são simplesmente casos particulares da soma e produto de cardinais, mediante a demonstração de que, de facto, a soma e produto de números naturais conduzem sempre a números naturais; estes factos podem ser facilmente demonstrados, por exemplo por indução. Podemos então encarar estas *operações* (ditas *binárias*) como *aplicações de $\mathbb{N} \times \mathbb{N}$ em \mathbb{N}* ; também podemos considerar deste modo a potência de base e expoente natural e já sabemos relacionar estas três operações, sendo o produto uma “*soma iterada*” e a potência um “*produto iterado*”, como se viu, em geral, para cardinais. As propriedades das operações que referimos para cardinais valem obviamente para números naturais, para além de outras propriedades conhecidas que nos dispensamos de recordar.

Outro conceito usual na aritmética dos inteiros é o de *subtração*; se $a \geq b$, $a, b \in \mathbb{N}$, demonstra-se que existe um e um só x tal que:

$$a = b + x$$

e x designa-se por *diferença* entre b e a , pondo-se:

$$x = a - b.$$

Não podemos afirmar que “ $-$ ” representa uma operação binária, uma vez que

existem pares de naturais (a, b) para os quais não se define $a - b$ (basta que $a < b$), não se tratando portanto de aplicação definida em $\mathbb{N} \times \mathbb{N}$. Referimos no final da secção 1 a conveniência em considerar dois “sinais” para os números em geral, para determinados efeitos; em particular em actividades como a contabilidade faz sentido considerar a “diferença” $a - b$ mesmo quando $a < b$, interpretando-se esse “valor” como $b - a$ “afectado do sinal menos”, no sentido em que, para repor a zero o saldo será necessário adicionar $b - a$ “à conta”. Pretender-se-ia então “estender” o conjunto \mathbb{N} de modo a que no novo conjunto, seja ele \mathbb{Z} , para qualquer elemento m existisse m' tal que:

$$m + m' = 0$$

(note-se que dados dois cardinais quaisquer a, b é fácil concluir que se $a + b = 0$, então $a = 0$ e $b = 0$). Um par ordenado $(\mathbb{Z}, +)$ em que $+$ é operação binária sobre \mathbb{Z} (ou seja, a correspondência $(m, n) \mapsto m + n$ é uma aplicação de $\mathbb{Z} \times \mathbb{Z}$ em \mathbb{Z}) designa-se por *grupóide*, sendo um dos exemplos mais elementares de *sistema algébrico*. Se a operação $+$ for *associativa* $(\mathbb{Z}, +)$ diz-se *semigrupo*; se além disso também for *comutativa*, diz-se semigrupo *comutativo*. Um elemento $0 \in \mathbb{Z}$ tal que:

$$\forall m \in \mathbb{Z}, 0 + m = m + 0 = m,$$

diz-se *elemento neutro* de $(\mathbb{Z}, +)$; é fácil verificar que, se existir, é único. Sendo $(\mathbb{Z}, +)$ *semigrupo com elemento neutro* 0 , se, além disso:

$$\forall m \in \mathbb{Z}, \exists m' \in \mathbb{Z} : m + m' = m' + m = 0,$$

$(\mathbb{Z}, +)$ diz-se *grupo*. Um elemento m' com a propriedade acima descrita diz-se *inverso* ou *simétrico* de m e também é fácil concluir que, se existir, é único, designando-se por $-m$; se para a operação se utilizar a “notação multiplicativa”, ou seja, mn ou $m \times n$ em lugar de $m + n$, é hábito representar o elemento neutro por 1 e o inverso de m por m^{-1} . É habitual reservar a notação aditiva para semigrupos *comutativos*.

De acordo com as definições anteriores, é fácil concluir que $(\mathbb{N}, +)$ e (\mathbb{N}, \cdot) são semigrupos comutativos, o primeiro com elemento neutro 0 , e que $(\mathbb{N} \setminus \{0\}, \cdot)$ é semigrupo comutativo com elemento neutro 1 ($\mathbb{N} \setminus \{0\}$ também se designa por \mathbb{N}_1). Pretendemos então “estender $(\mathbb{N}, +)$ a um grupo $(\mathbb{Z}, +)$ ” (dito “*grupo dos inteiros relativos*”, ou simplesmente “*grupo dos inteiros*”), com os abusos de linguagem evidentes; supondo que tínhamos conseguido o nosso propósito, então, dados $m, n \in \mathbb{N}$ quaisquer, teríamos, em \mathbb{Z} :

$$m = 0 + m = (n + (-n)) + m = n + ((-n) + m) = n + (m + (-n)),$$

pelo que, estendendo a \mathbb{Z} a definição usual de subtracção em \mathbb{N} :

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

Ou seja, teríamos resolvido o problema de definir a diferença de quaisquer dois números naturais; além disso aplicando raciocínios análogos a quaisquer $m, n \in \mathbb{Z}$, vemos que conseguimos “transformar a subtracção numa operação binária”, agora em \mathbb{Z} . Deste modo, quaisquer dois números naturais m, n dão

lugar ao número inteiro $m - n$, mas esta correspondência não é *biunívoca*, mesmo que supuséssemos \mathbb{Z} apenas composto por diferenças deste tipo, ou seja, mesmo que “reduzíssemos” \mathbb{Z} apenas à imagem da aplicação, definida em $\mathbb{N} \times \mathbb{N}$, $(m, n) \mapsto m - n$ (\mathbb{Z} continuaria a ser um grupo aditivo, como é fácil concluir). Com efeito tal aplicação *não é injectiva*, uma vez que, para todos os pares $(m, n), (m', n') \in \mathbb{N} \times \mathbb{N}$:

$$(m - n = m' - n') \Leftrightarrow (m + n' = m' + n),$$

e a condição $m + n' = m' + n$ não obriga a que $m = m', n = n'$, como é fácil concluir. No entanto podemos facilmente verificar que a relação \sim entre pares de números naturais dada precisamente por:

$$(m, n) \sim (m', n') \text{ sse } m + n' = m' + n,$$

é *de equivalência*; como todas as relações de equivalência num conjunto, determina em $\mathbb{N} \times \mathbb{N}$ uma chamada *partição*, ou seja, uma parte de $\mathcal{P}(\mathbb{N} \times \mathbb{N})$ constituída por conjuntos dois a dois disjuntos, não vazios, e cuja união é igual a $\mathbb{N} \times \mathbb{N}$, sendo cada um desses conjuntos, neste caso, a chamada “*classe de equivalência*” de um elemento (m, n) de $\mathbb{N} \times \mathbb{N}$ (ou seja, o conjunto dos elementos de $\mathbb{N} \times \mathbb{N}$ que estão na relação \sim com (m, n) , que representaremos por $[(m, n)]$). Tal *partição* designa-se por *conjunto quociente de $\mathbb{N} \times \mathbb{N}$ pela relação de equivalência \sim* e representa-se por:

$$(\mathbb{N} \times \mathbb{N})/\sim.$$

A relação \sim foi definida a partir da aplicação “diferença” de $\mathbb{N} \times \mathbb{N}$ para \mathbb{Z} (já reduzido de modo a que esta aplicação ficasse sobrejectiva), determinando a “equivalência” dos pares com a mesma imagem; sempre que se define uma “equivalência” deste modo, é fácil concluir que é possível definir também uma aplicação “quociente” do conjunto quociente (neste caso $(\mathbb{N} \times \mathbb{N})/\sim$) sobre a imagem da aplicação inicial, tomando para imagem de cada classe de equivalência a imagem através da aplicação inicial de um elemento qualquer da classe. Esta aplicação quociente fica agora *bijectiva*. Ou seja, se supuséssemos que tínhamos encontrado o grupo $(\mathbb{Z}, +)$ com as condições requeridas e o “menor possível”, ou seja, restringindo-o às “diferenças de números naturais”, poderíamos concluir que estava em correspondência biunívoca com os elementos de:

$$(\mathbb{N} \times \mathbb{N})/\sim$$

através da aplicação de $(\mathbb{N} \times \mathbb{N})/\sim$ em \mathbb{Z} :

$$[(m, n)] \mapsto m - n$$

(definida para cada classe de equivalência $[(m, n)]$, com $m, n \in \mathbb{N}$). Vejamos como se comporta a aplicação inversa com a operação de soma definida em \mathbb{Z} ; como é fácil ver,

$$(m - n) + (m' - n') = (m + m') - (n + n'),$$

para quaisquer $m, n, m', n' \in \mathbb{N}$, pelo que a soma dos inteiros $m - n$ e $m' - n'$ será imagem pela referida bijecção da classe de equivalência:

$$[(m + m', n + n')].$$

Esta observação sugere que se defina em $(\mathbb{N} \times \mathbb{N})/\sim$ uma operação designada por *soma* e definida por:

$$[(m, n)] + [(m', n')] = [(m + m', n + n')] \quad (2^3);$$

se assim fizermos, a bijecção estabelecida entre $(\mathbb{N} \times \mathbb{N})/\sim$ e \mathbb{Z} terá a propriedade notável de “*transformar a soma em $(\mathbb{N} \times \mathbb{N})/\sim$ na soma em \mathbb{Z}* ”, ou seja, tratar-se-á de *isomorfismo* entre os grupóides $((\mathbb{N} \times \mathbb{N})/\sim, +)$ e $(\mathbb{Z}, +)$, o que tornaria $((\mathbb{N} \times \mathbb{N})/\sim, +)$ também um grupo, como seria fácil concluir, caso $(\mathbb{Z}, +)$ existisse de facto. Além disso, à classe $[(m, n)]$ corresponde um número natural sse $m \geq n$, pelo que esta propriedade caracteriza os elementos de $(\mathbb{N} \times \mathbb{N})/\sim$ que correspondem aos números naturais no isomorfismo; satisfeita a condição $m \geq n$, $m - n$ também será elemento de \mathbb{N} , pelo que:

$$(m, n) \sim (m - n, 0)$$

e a parte de $(\mathbb{N} \times \mathbb{N})/\sim$ que corresponde a \mathbb{N} será assim constituída exactamente pelas classes $[(n, 0)]$ com $n \in \mathbb{N}$, uma vez que $n = n - 0$ e portanto os “ $m - n$ com $m \geq n$ ” são afinal todos os $n \in \mathbb{N}$.

Estas considerações mostram que, caso o nosso “problema” tenha solução, esta terá de ser um grupóide isomorfo a $((\mathbb{N} \times \mathbb{N})/\sim, +)$; ora é fácil verificar que este grupóide é, de facto, grupo, com elemento neutro:

$$[(0, 0)]$$

e tal que, para cada $m, n \in \mathbb{N}$,

$$-[(m, n)] = [(n, m)].$$

Além disso, a aplicação $n \mapsto [(n, 0)]$ é um *isomorfismo* do semigrupo com elemento neutro $(\mathbb{N}, +)$ sobre a respectiva imagem em $((\mathbb{N} \times \mathbb{N})/\sim, +)$. Se *passarmos a considerar* que \mathbb{N} é esta parte de $((\mathbb{N} \times \mathbb{N})/\sim, +)$ constituída pelas classes $[(n, 0)]$ com $n \in \mathbb{N}$, todas as propriedades algébricas envolvendo a soma de números naturais se transferem para o novo conjunto que está assim em correspondência biunívoca com \mathbb{N} . Neste caso, o próprio grupo $((\mathbb{N} \times \mathbb{N})/\sim, +)$ é solução do problema que nos tínhamos proposto resolver, em relação ao “novo” conjunto de números naturais que acabámos de definir²⁴; passaremos então a designá-lo, naturalmente, por $(\mathbb{Z}, +)$. Notemos que, pelas definições anteriores:

$$\begin{aligned} [(m, n)] &= [(m, 0) + (0, n)] = [(m, 0)] + [(0, n)] = [(m, 0)] + (-[(n, 0)]) = \\ &= [(m, 0)] - [(n, 0)], \end{aligned}$$

pelo que os números interiores são, de facto, diferenças de números naturais; como

²³Por abuso de linguagem, representámos a operação pelo mesmo símbolo já utilizado para a operação em \mathbb{Z} , a qual já era, aliás, extensão da adição em \mathbb{N} .

²⁴Se preferirmos, podemos substituir em $(\mathbb{N} \times \mathbb{N})/\sim$ cada $[(n, 0)]$ por n , fazendo o mesmo na operação $+$, entendida como conjunto de pares ordenados; nesse caso os números naturais continuarão a ser os nossos “conhecidos”...

para cada $m, n \in \mathbb{N}$ se tem $m \geq n$ ou $n \geq m$, teremos sempre $[(m, n)] = [(m - n, 0)]$ ou $[(m, n)] = [(0, m - n)] = -[(m - n, 0)]$, com $m - n \in \mathbb{N}$, pelo que qualquer inteiro será igual a um número natural p ou ao simétrico $-p$ de um número natural. Em particular, podemos representar qualquer inteiro negativo $-n$ ($n \in \mathbb{N}$) em determinada base B , simplesmente antepondo à representação de n o sinal “-”.

Procuremos agora estender o produto de números naturais a \mathbb{Z} ; comecemos por notar que em qualquer semigrupo (\mathbb{G}, \oplus) com elemento neutro, para cada $n \in \mathbb{N}$ podemos definir por recorrência (método de definição que se baseia no Princípio de Indução) a operação *unária* (ou seja, uma aplicação de \mathbb{G} em \mathbb{G}), dita “*n-múltiplo*”:

$$g \mapsto ng,$$

pondo:

$$\begin{cases} 0g = \mathbb{O} \\ (n+1)g = ng \oplus g, \end{cases}$$

onde \mathbb{O} é o elemento neutro do semigrupo²⁵. No caso de utilizarmos a notação multiplicativa, representando o elemento neutro por \mathbb{I} , e a operação do semigrupo por \otimes , a operação “*n-múltiplo*” designa-se habitualmente por “*potência de expoente n*” e representa-se por:

$$g^n$$

(ou seja, $g^0 = \mathbb{I}$, $g^{(n+1)} = g^n \otimes g$). No caso em que (\mathbb{G}, \oplus) é *grupo* podemos estender a definição a $n \in \mathbb{Z}$; basta definir o “*-n-múltiplo*” (ou, em notação multiplicativa, a “*potência de expoente -n*”) para $n \in \mathbb{N}_1$, através de:

$$(-n)g = -(ng)$$

(ou seja, em notação multiplicativa, $g^{-n} = (g^n)^{-1}$). É fácil demonstrar, por indução, as propriedades elementares dos múltiplos (ou, de modo equivalente, das potências); por exemplo:

$$(m+n)g = mg \oplus ng, m(ng) = (mn)g, m\mathbb{O} = \mathbb{O}$$

(ou seja, $g^{m+n} = g^m \otimes g^n$, $(g^n)^m = g^{mn}$, $\mathbb{I}^m = \mathbb{I}$). Se (\mathbb{G}, \oplus) for *comutativo* (o que também se chama *grupo abeliano*), teremos também:

$$m(g \oplus h) = mg \oplus mh$$

(ou seja, $(g \otimes h)^m = g^m \otimes h^m$). Em particular, podemos aplicar estas definições e propriedades ao grupo aditivo abeliano dos inteiros, o que permite definir a *multiplicação em \mathbb{Z}* , entendido como grupo aditivo, ou seja, o *produto de dois números inteiros* m, n (representado por $m.n$ ou por mn) através do *m-múltiplo de n*. As propriedades dos múltiplos implicam facilmente que $(\mathbb{Z}, .)$ (representando a multiplicação por “.”) é semigrupo comutativo com elemento neutro 1; com

²⁵Se (\mathbb{G}, \oplus) não tivesse elemento neutro também poderíamos definir o *n-múltiplo* para qualquer $n \in \mathbb{N}_1$, pondo $1g = g$ e, do mesmo modo, $(n+1)g = ng \oplus g$.

efeito, por exemplo:

$$1.n = (0 + 1)n = 0n + n = 0 + n = n$$

e também se demonstra facilmente que $n.1 = n$, uma vez que $0.1 = 0$, por definição e se, por hipótese, $n.1 = n$, então:

$$(n + 1).1 = n.1 + 1 = n + 1.$$

Podemos agora considerar a *estrutura algébrica* $(\mathbb{Z}, +, \cdot)$; sabemos que $(\mathbb{Z}, +)$ é *grupo abeliano*, que (\mathbb{Z}, \cdot) é *semigrupo*, e que a *multiplicação é distributiva em relação à adição à direita e à esquerda*, atendendo às propriedades dos múltiplos. Estas propriedades resumem-se dizendo que $(\mathbb{Z}, +, \cdot)$ é *Anel*, neste caso *comutativo*, uma vez que o *produto* é comutativo, e *com unidade*, uma vez que existe elemento neutro para a multiplicação.

Pretendemos agora estender a ordem de \mathbb{N} a \mathbb{Z} ; notemos que, dados $m, n \in \mathbb{N}$,

$$m \geq n \Leftrightarrow m - n \in \mathbb{N} \Leftrightarrow m - n \geq 0.$$

Obteremos assim uma relação em \mathbb{Z} , que estende a ordem em \mathbb{N} , definindo $m \geq n$ para cada $m, n \in \mathbb{Z}$ ⁽²⁶⁾ através de:

$$m - n \in \mathbb{N};$$

ora, é fácil concluir que relação assim definida em \mathbb{Z} é, de facto, de ordem total (lata). Em particular, teremos, para todo o $n \in \mathbb{Z}$:

$$n \in \mathbb{N} \Leftrightarrow n - 0 \in \mathbb{N} \Leftrightarrow n \geq 0,$$

e portanto, $n \in \mathbb{Z} \setminus \mathbb{N}$ sse $n < 0$; costuma designar-se $\mathbb{Z} \setminus \mathbb{N}$ por \mathbb{Z}^- (“conjunto dos inteiros negativos”) sendo constituído pelo $-n$ com $n \in \mathbb{N}_1$, ou seja:

$$\mathbb{Z} = \mathbb{Z}^- \cup \mathbb{N} = \mathbb{Z}^- \cup \{0\} \cup \mathbb{N}_1.$$

Esta relação satisfaz além disso às seguintes propriedades:

$$\forall m, n, p \in \mathbb{Z}, m \geq n \Rightarrow m + p \geq n + p,$$

e,

$$\forall m, n \in \mathbb{Z}, m, n > 0 \Rightarrow mn > 0,$$

o que se exprime dizendo que $(\mathbb{Z}, +, \cdot, \leq)$ é *Anel ordenado*. Em particular, ter-se-á, como é fácil concluir,

$$\bullet m > 0 \text{ sse } -m < 0$$

e:

$$\bullet mn > 0 \text{ sse } ((m > 0 \text{ e } n > 0) \text{ ou } (m < 0 \text{ e } n < 0)).$$

Do que precede podemos concluir que, dados $m, n \in \mathbb{Z}$, $m < n$ sse se verificar uma das seguintes três condições:

²⁶Por abuso de linguagem, utilizaremos o mesmo símbolo para representar a nova relação em \mathbb{Z} .

- $m \notin \mathbb{N}$ e $n \in \mathbb{N}$ (ou seja, m é “negativo” e n é “positivo ou nulo”)
- $m, n \in \mathbb{N}$ e $m < n$ em \mathbb{N}
- $m, n \notin \mathbb{N}$ e $-n < -m$ em \mathbb{N} .

Deste modo podemos sempre utilizar os sinais e os algarismos da representação de dois números inteiros quaisquer para determinar qual dos dois é maior, utilizando eventualmente o critério enunciado para números naturais.

Considerando a sucessão $0, 1, -1, 2, -2, \dots, n, -n, \dots$ cuja definição formal é deixada ao leitor, facilmente se conclui que \mathbb{Z} é equipotente a \mathbb{N} , pelo que:

$$\#\mathbb{Z} = \aleph_0.$$

11. Divisão em \mathbb{Z} . O corpo \mathbb{Q} das fracções de \mathbb{Z} ou dos números racionais.

Definimos na secção 4 a divisão inteira para quaisquer $a, b \in \mathbb{N}$ tais que $b \neq 0$, dando lugar a um par bem determinado de números inteiros, (q, r) , sendo q o quociente e r o resto. Poderíamos agora fundamentar plenamente as propriedades da divisão, utilizando em particular o princípio de boa ordenação; no caso particular em que $r = 0$, as ideias heurísticas que levaram à introdução das fracções racionais conduzem a:

$$\frac{a}{b} = q,$$

mas, tal como no caso da subtracção, não podemos considerar a correspondência

$$(a, b) \mapsto \frac{a}{b}$$

como operação em \mathbb{N} , uma vez que não fica assim definida para todos os pares de $\mathbb{N} \times \mathbb{N}$, mas apenas para o pares (a, b) tais que o resto da divisão de a por b é igual a zero. No caso em que $a, b \in \mathbb{Z}$, podemos também, por vezes, definir a/b (ou $a \div b$) como sendo o inteiro q , no caso em que existe, tal que:

$$a = qb,$$

uma vez que q é único, caso exista, como é fácil verificar através das propriedades elementares da multiplicação em \mathbb{Z} . As propriedades heurísticas das fracções sugerem que, em qualquer caso, uma vez definida a fracção a/b teremos também:

$$a = \frac{a}{b} b,$$

e, em particular, se $b \neq 0$,

$$\frac{1}{b} b = 1 = b \frac{1}{b}, \quad \frac{a}{b} = a \frac{1}{b},$$

ou seja, a/b será igual ao produto ab^{-1} , onde, como é habitual, representamos por b^{-1} o inverso de b para a operação “.” “estendida às fracções racionais”. Deste

modo, construir as fracções racionais (positivas ou negativas) é equivalente a estender as operações do anel $(\mathbb{Z}, +, \cdot)$ a certo conjunto \mathbb{Q} (“o menor possível”), de maneira que $(\mathbb{Q}, +, \cdot)$ seja anel comutativo e $(\mathbb{Q} \setminus \{0\}, \cdot)$ seja grupo; tal anel dir-se-á então um *corpo* que designaremos por corpo dos *números racionais* ou das *fracções racionais*. Com análise análoga à desenvolvida para a construção de \mathbb{Z} , admitindo que tal corpo existe, sejam então $a, b \in \mathbb{Z}, b \neq 0$; teríamos:

$$a = a \cdot 1 = a \cdot (b^{-1}b) = (a \cdot b^{-1})b,$$

pelo que, estendendo a \mathbb{Q} a noção habitual de quociente em \mathbb{Z} , viria:

$$\frac{a}{b} = ab^{-1}.$$

Também neste caso seria fácil concluir que restringindo \mathbb{Q} aos quocientes a/b deste tipo (ou seja, com $a, b \in \mathbb{Z}, b \neq 0$) ainda teríamos um corpo estendendo \mathbb{Z} (uma vez que $a = a/1$, se $a \in \mathbb{Z}$), pelo que \mathbb{Q} deverá ser constituído apenas por estes quocientes, uma vez que pretendemos que seja o menor possível. Cada número racional ficará então associado a um par (a, b) de números inteiros tais que $b \neq 0$, mas, tal como na construção de \mathbb{Z} , esta correspondência não é biunívoca; com efeito:

$$\begin{aligned} \frac{a}{b} = \frac{a'}{b'} &\Leftrightarrow ab^{-1} = a'b'^{-1} \Leftrightarrow \\ &\Leftrightarrow (b^{-1}a)b' = (ab^{-1})b' = (a'b'^{-1})b' = a'(b'^{-1}b') = a'1 = a' \\ &\Leftrightarrow ab' = 1(ab') = (bb^{-1})(ab') = b((b^{-1}a)b') = ba' \end{aligned}$$

e, como é fácil concluir, a condição $ab' = ba'$ não implica que $a = a'$ e $b = b'$. Somos assim conduzidos a introduzir em $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ uma relação de equivalência \approx através de:

$$(a, b) \approx (a', b') \text{ sse } ab' = ba',$$

e, de modo análogo ao que acima se concluiu para a relação \sim em $\mathbb{N} \times \mathbb{N}$, a aplicação $(a, b) \mapsto ab^{-1}$ de $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ em \mathbb{Q} determina uma bijecção do conjunto quociente

$$\mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) / \approx$$

sobre \mathbb{Q} , através de:

$$[(a, b)] \mapsto ab^{-1}.$$

Vejamos como se comporta a aplicação inversa com as operações definidas em \mathbb{Q} ; para o produto temos:

$$(ab^{-1}) \cdot (a'b'^{-1}) = (aa')(b^{-1}b'^{-1}) = (aa')(b'b)^{-1} = (aa')(bb')^{-1},$$

pelo que este produto é a imagem da classe $[(aa', bb')]$ pela referida bijecção. Relativamente à soma temos:

$$\begin{aligned} ab^{-1} + a'b'^{-1} &= (ab^{-1})(b'b'^{-1}) + (a'b'^{-1})(bb^{-1}) = \\ &= (ab')(bb')^{-1} + (a'b)(bb')^{-1} = (ab' + a'b)(bb')^{-1}, \end{aligned}$$

o que torna esta soma imagem pela bijecção da classe $[(ab' + a'b, bb')]$. Deste modo, se o corpo $(\mathbb{Q}, +, \cdot)$ existisse, definindo em $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})/\approx$ as operações de adição e multiplicação através de:

$$\begin{cases} [(a, b)] + [(a', b')] = [(ab' + a'b, bb')] \\ [(a, b)] \cdot [(a', b')] = [(aa', bb')], \end{cases}$$

a bijecção acima definida seria isomorfismo de anéis, o que tornaria $((\mathbb{Z} \times (\mathbb{Z} \setminus \{0\}))/\approx, +, \cdot)$ corpo; nesse isomorfismo, aos inteiros corresponderiam as classes da forma $[(a, 1)]$. Podemos então definir:

$$\mathbb{Q} = \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})/\approx$$

com as operações acima introduzidas e é fácil verificar que $(\mathbb{Q}, +, \cdot)$ é corpo, sendo $[(0, 1)]$ o elemento neutro da adição, $[(1, 1)]$ o elemento neutro da multiplicação, para cada $[(a, b)] \in \mathbb{Q}$:

$$-[(a, b)] = [(-a, b)]$$

e se $[(a, b)] \neq [(0, 1)]$ então:

$$[(a, b)]^{-1} = [(b, a)].$$

Além disso é isomorfismo (de anéis) sobre a imagem a aplicação de \mathbb{Z} em \mathbb{Q} dada por:

$$a \mapsto [(a, 1)].$$

Agora, dados $a, b \in \mathbb{Z}, b \neq 0$, temos:

$$[(a, b)] = [(a \cdot 1, 1 \cdot b)] = [(a, 1)] \cdot [(1, b)] = [(a, 1)] \cdot [(b, 1)]^{-1} = a/b,$$

se identificarmos cada $a \in \mathbb{Z}$ com a respectiva imagem no isomorfismo que acabamos de estabelecer⁽²⁷⁾. Assim, tal com prevíamos, \mathbb{Q} é exactamente constituído pelas “fracções racionais” de numerador e denominador inteiros.

Procuremos agora estender a \mathbb{Q} a ordem de \mathbb{Z} ; se pretendermos que com essa ordem, além disso, se obtenha um anel (neste caso corpo) ordenado, deverá ter-se, para $r \in \mathbb{Q} \setminus \{0\}$:

$$rr^{-1} = 1 > 0,$$

donde:

$$(r > 0 \text{ e } r^{-1} > 0) \text{ ou } (r < 0 \text{ e } r^{-1} < 0).$$

²⁷ De modo análogo ao que se referiu na construção de \mathbb{Z} , também poderíamos substituir em \mathbb{Q} as imagens dos inteiros no isomorfismo pelos correspondentes inteiros, efectuando idêntica substituição nas operações, o que tornaria, deste modo, \mathbb{Q} “verdadeira” extensão de \mathbb{Z} .

Em particular, dados $a, b \in \mathbb{Z}$, $b \neq 0$, como $a/b = ab^{-1}$, teremos $a/b > 0$ sse a e b “tiverem o mesmo sinal”, uma vez que acabámos de concluir que b e b^{-1} deverão ter sempre o mesmo sinal. Deste modo, a existir a ordem pretendida, deverá satisfazer a esta condição; agora é fácil verificar que com a relação \leq a ela associada em \mathbb{Q} se obtém, de facto, um corpo ordenado, ou seja, começamos por definir $a/b > 0$, como acima (a e b têm o mesmo sinal) e agora, dados $r, r' \in \mathbb{Q}$, basta pôr, por definição:

$$r \leq r' \text{ sse } (r = r' \text{ ou } r' - r > 0).$$

Como é de esperar designam-se por \mathbb{Q}^+ e \mathbb{Q}^- os conjuntos dos racionais, respectivamente maiores e menores que zero.

Poderíamos agora justificar rigorosamente os raciocínios efectuados para obter a representação dos números racionais em sistema posicional em determinada base. Deste modo, fixado um número natural $B > 1$, podemos estabelecer uma bijecção entre \mathbb{Q}^+ e o conjunto dos pares (a, d) em que a é uma sequência finita (a_0, \dots, a_k) ($k \in \mathbb{N}$) de números inteiros no intervalo $[0, B - 1]$, sendo $a_k > 0$, e d uma sucessão $(d_n)_{n \in \mathbb{N}_1}$ também de números inteiros no intervalo $[0, B - 1]$, para a qual existem $j_0 \in \mathbb{N}$, $p \in \mathbb{N}_1$, tais que, para qualquer $q \in \{1, \dots, p\}$, $m \in \mathbb{N}$:

$$d_{j_0+q+mp} = d_{j_0+q}$$

de maneira que, no caso $p = 1$, não se tenha $d_{j_0+1} = B - 1$. Nessa bijecção, ao par (a, d) corresponde o número racional:

$$\sum_{j=0}^k a_j B^j + \sum_{n \in \mathbb{N}_1} d_n \frac{1}{B^n}.$$

O par (a, d) (ou o número racional que lhe está associado através da referida bijecção) representa-se habitualmente por:

$$(\alpha_k \dots \alpha_0, \delta_1 \dots \delta_{j_0} (\delta_{j_0+1} \dots \delta_{j_0+p}))_B$$

ou, quando não houver perigo de confusão, simplesmente por:

$$\alpha_k \dots \alpha_0, \delta_1 \dots \delta_{j_0} (\delta_{j_0+1} \dots \delta_{j_0+p})$$

sendo, para cada $j = 0, \dots, k$, α_j o algarismo representativo de a_j e, para cada $n = 1, \dots, j_0 + p$, δ_n o algarismo representativo de d_n . É habitual omitir-se o “parte periódica da dízima”, ou seja, $(\delta_{j_0+1} \dots \delta_{j_0+p})$, quando esta se reduz a (0) , e, como é óbvio, convencionam-se que $\delta_1 \dots \delta_{j_0}$ representa o “símbolo vazio” (“é omitido”) quando $j_0 = 0$. Para obter a representação dos elementos de \mathbb{Q}^- , basta, obviamente, acrescentar à esquerda o sinal “−” à representação dos respectivos simétricos.

Através destas bijecções poderíamos agora identificar os números racionais com um conjunto incluindo os pares (a, d) que acabámos de definir, sendo os negativos identificados com os pares “afectados de sinal”, por qualquer processo que permita distinguir uns dos outros – invertendo o par, por exemplo – e

acrescentando o zero, e poderíamos mesmo introduzir neste conjunto as operações de adição e multiplicação utilizando os algoritmos conhecidos destas operações, adaptados, naturalmente, às “dígitas finitas ou periódicas”.

O modo como \mathbb{Q} foi construído permite concluir, sem dificuldade, que:

$$\#\mathbb{Q} \leq \#(\mathbb{Z} \times \mathbb{Z}) = \aleph_0 \cdot \aleph_0 = \aleph_0,$$

pelo que, obviamente:

$$\#\mathbb{Q} = \aleph_0,$$

embora também seja fácil provar que situado estritamente entre dois racionais existe sempre um racional.

12. Sucessões de Cauchy em \mathbb{Q} . O corpo \mathbb{R} dos números reais.

Verificámos na secção 1 que, dado um número inteiro positivo a , nem sempre era possível encontrar r racional tal que:

$$r^2 = a;$$

quando tal r existisse designar-se-ia por *raiz quadrada de a* , representando-se por:

$$\sqrt{a}.$$

Conceito análogo pode ser introduzido substituindo o expoente 2 por qualquer número natural $q > 0$; designar-se-á por *raiz q -ésima de a* (*raiz cúbica, raiz quarta, etc.*), ou *raiz de índice q de a* , representando-se por:

$$\sqrt[q]{a},$$

e teremos, por definição, para qualquer inteiro p :

$$((\sqrt[q]{a})^p)^q = (\sqrt[q]{a})^{pq} = ((\sqrt[q]{a})^q)^p = a^p \Rightarrow (\sqrt[q]{a})^p = \sqrt[q]{a^p},$$

o que motiva a definição de *potência de expoente fraccionário p/q* ; com efeito, se pretendermos manter as regras das operações envolvendo expoentes, teremos, nos casos em que faz sentido:

$$(a^{\frac{p}{q}})^q = a^{\frac{p}{q}q} = a^p,$$

pelo que, por definição, terá de ser:

$$a^{\frac{p}{q}} = \sqrt[q]{a^p} = (\sqrt[q]{a})^p.$$

Será possível estender o corpo \mathbb{Q} a um corpo \mathbb{R} (também “o menor possível”) onde seja sempre possível extrair a raiz de índice q de um número não negativo, ou, de modo idêntico, definir sempre a respectiva potência de expoente fraccionário? Verificámos nas secções 4 e 5 que esta questão está associada à possibilidade de interpretar como “números” as chamadas “dígitas infinitas não periódicas”, as quais definem sucessões de somas (séries) que, não sendo convergentes em \mathbb{Q} ,

têm a propriedade notável que as torna no que chamamos *sucessões de Cauchy*. De maneira geral, diremos que uma sucessão $(x_n)_{n \in \mathbb{N}_1}$ de números racionais é de *Cauchy* se para qualquer $\delta > 0$ existir $p \in \mathbb{N}_1$ tal que, para todos os $m, n \in \mathbb{N}_1$,

$$m, n \geq p \Rightarrow |x_m - x_n| < \delta.$$

Se pensarmos na representação posicional em determinada base dos termos de tal sucessão, é fácil concluir que, fixado $k \in \mathbb{N}_1$, a partir de certa ordem os termos da sucessão têm o algarismo todos respectivamente iguais, até à ordem k da “parte decimal”, pelo que tal sucessão define de maneira única uma “representação posicional” na mesma base, eventualmente “infinita não periódica” (sê-lo-á exactamente se a sucessão de Cauchy não convergir para um número racional) e eventualmente afectada do sinal “-”. Podemos assim estabelecer uma correspondência entre o conjunto das sucessões de Cauchy de números racionais e o conjunto das representações posicionais “em geral” (com o respectivo sinal), mas, como é fácil suspeitar, não é biunívoca, uma vez que a uma mesma “díizima” podem corresponder diversas sucessões de Cauchy que lhe dão origem (basta que a diferença entra a sucessão de Cauchy e a série associada à “díizima” convirja para zero). A análise que se fez na secção 5 do algoritmo da raiz quadrada demonstra que se pode obter sempre uma sucessão de Cauchy de números racionais cujo quadrado converge para determinado racional $p > 0$; raciocínio idêntico poderia ter sido feito em geral para a raiz q -ésima, o que associa o problema da potenciação de expoente fraccionário ao da convergência das sucessões de Cauchy e, atendendo ao que acabámos de observar, ao da interpretação das “díizimas” (finitas, ou infinitas periódicas ou não periódicas) como números de “espécie” mais geral que os racionais.

Analogamente ao que acima fizémos para a construção de \mathbb{Z} e \mathbb{Q} , suponhamos que existe um corpo ordenado $(\mathbb{R}, +, \cdot, \leq)$ (dito *dos números reais*) estendendo $(\mathbb{Q}, +, \cdot, \leq)$, o menor possível, e no qual as sucessões de Cauchy tenham sempre limite; então, em particular, tal corpo conterá os limites de todas as sucessões de Cauchy de números racionais. Atendendo às propriedades básicas das sucessões de Cauchy e da noção de limite de sucessão, não seria difícil concluir que esse conjunto dos limites de sucessões de Cauchy de números racionais constitui sub-corpo ordenado de $(\mathbb{R}, +, \cdot, \leq)$ onde todas as sucessões de Cauchy ainda têm limite, pelo que podemos restringir \mathbb{R} a esse conjunto, uma vez que pretendemos que seja o menor possível. Deste modo podemos definir uma aplicação sobrejectiva entre o conjunto \mathcal{S} das sucessões de Cauchy de números racionais e \mathbb{R} que associa a cada sucessão de \mathcal{S} o respectivo limite em \mathbb{R} ; não se trataria de bijecção, uma vez que, dadas duas sucessões de Cauchy de números racionais, $(x_n)_{n \in \mathbb{N}_1}, (y_n)_{n \in \mathbb{N}_1}$, convergindo para determinados números reais, respectivamente x e y , teremos:

$$x = y \text{ sse } x_n - y_n \xrightarrow[n]{} 0.$$

Analogamente ao que se fez na construção de \mathbb{Z} e \mathbb{Q} , podemos agora definir em \mathcal{S} uma relação, que facilmente se conclui ser de equivalência, por:

$$(x_n)_{n \in \mathbb{N}_1} \simeq (y_n)_{n \in \mathbb{N}_1} \text{ sse } x_n - y_n \xrightarrow[n]{} 0;$$

tal como nas referidas situações, também agora se obtém uma bijecção entre o conjunto quociente $\mathcal{S}_{/\simeq}$ e \mathbb{R} a partir da sobrejecção que acabámos de definir. Examinando o comportamento da bijecção inversa, facilmente se vê que se tratará de um isomorfismo de anéis ordenados desde que se definam as operações e a ordem em $\mathcal{S}_{/\simeq}$ através de:

$$\begin{cases} [(x_n)_{n \in \mathbb{N}_1}] + [(y_n)_{n \in \mathbb{N}_1}] = [(x_n + y_n)_{n \in \mathbb{N}_1}] \\ [(x_n)_{n \in \mathbb{N}_1}] \cdot [(y_n)_{n \in \mathbb{N}_1}] = [(x_n \cdot y_n)_{n \in \mathbb{N}_1}], \\ [(x_n)_{n \in \mathbb{N}_1}] < [(y_n)_{n \in \mathbb{N}_1}] \text{ sse } (x_n - y_n) \not\rightarrow_n 0 \text{ e } \exists k \in \mathbb{N}_1 : \forall n \geq k, x_n < y_n. \end{cases}$$

Deste modo, se $(\mathbb{R}, +, \cdot, \leq)$ existir, terá de ser isomorfo a $(\mathcal{S}_{/\simeq}, +, \cdot, \leq)$; além disso, nesse isomorfismo, aos números racionais corresponderão exactamente as classes $[(x_n)_{n \in \mathbb{N}_1}]$ onde $(x_n)_{n \in \mathbb{N}_1}$ é sucessão de Cauchy de números racionais convergente em \mathbb{Q} , e os elementos de $\mathcal{S}_{/\simeq}$ serão todos limites de sucessões de elementos correspondentes a números racionais no referido isomorfismo. Restará então provar que $(\mathcal{S}_{/\simeq}, +, \cdot, \leq)$ é, de facto, corpo ordenado e que todas as sucessões de Cauchy convergem em $\mathcal{S}_{/\simeq}$ (ou seja que $(\mathcal{S}_{/\simeq}, +, \cdot, \leq)$ é *corpo ordenado completo*); podemos, se o desejarmos, substituir em $\mathcal{S}_{/\simeq}$ (e nas operações e relação de ordem) as classes correspondentes a números racionais pelos respectivos elementos de \mathbb{Q} , o que termina a construção dos números reais, com as propriedades requeridas, sendo a solução única a menos de isomorfismo de anéis ordenados; também se poderia agora mostrar que, a menos de isomorfismo, $(\mathbb{R}, +, \cdot, \leq)$ é o único *corpo ordenado completo*. Notemos finalmente que a correspondência que acima considerámos entre sucessões de Cauchy de números racionais e representações posicionais em determinada base (incluindo as dízimas não periódicas) define uma bijecção entre $\mathcal{S}_{/\simeq}$ (ou seja, \mathbb{R}) e essas representações (afectadas do respectivo sinal). Seria agora possível justificar plenamente a existência da raiz q -ésima de qualquer real não negativo x , bastando construir uma sucessão de Cauchy cuja potência q convirja para x (como se fez para o caso $q = 2$ na secção 5), e verificar em seguida que o limite dessa sucessão de Cauchy tem exactamente potência q igual a x (trata-se, por outras palavras, de provar a *continuidade da função* $t \mapsto t^q$ de \mathbb{R} em \mathbb{R} e utilizar a unicidade do limite).

Que se poderá dizer acerca do número de elementos de \mathbb{R} ? se pensarmos apenas nos números reais estritamente situados entre 0 e 1, pelo que atrás vimos, este conjunto ficará em correspondência biunívoca com as respectivas representações posicionais na base 2, por exemplo. Estas, por sua vez, correspondem às sucessões $(x_n)_{n \in \mathbb{N}_1}$ onde $x_n = 0$ ou $x_n = 1$, excluindo a sucessão identicamente nula e as que sejam constantes iguais a 1 a partir de certa ordem; as sucessões que excluímos constituem um conjunto *numerável*, como é fácil concluir e a totalidade das sucessões daquele tipo constituem o conjunto:

$$\{0, 1\}^{\mathbb{N}_1},$$

com cardinal, por definição, igual a:

$$2^{\aleph_0} = \aleph_1.$$

Daqui se conclui facilmente que o conjunto dos reais entre 0 e 1 tem cardinal \aleph_1 ; como \mathbb{R} é união *numerável* de conjuntos equipotentes a este, não seria difícil concluir que:

$$\#\mathbb{R} = \aleph_1 > \aleph_0 = \#\mathbb{Q} = \#\mathbb{Z} = \#\mathbb{N}.$$

Poderíamos agora regressar à interpretação geométrica dos números reais, baseando-nos em alguma das axiomáticas da Geometria Euclidiana; Hilbert, por exemplo, introduz axiomáticamente a noção de congruência de segmentos que permite efectuar a construção dos reais positivos como classe de equivalência de segmentos congruentes no plano ou no espaço, fixado um segmento-unidade e, a partir daí, construir um corpo ordenado partindo de uma recta em que se fixe uma origem e um sentido, com as operações definidas geometricamente. Deste modo fica estabelecida uma bijecção entre o corpo dos reais e os pontos dessa recta, a qual também se passa a chamar a “*recta real*”.

BIBLIOGRAFIA

- BOURBAKI, N., Elements of Mathematics, Theory of Sets, Hermann, Paris, 1967
- GUERREIRO, J. S., Curso de Matemáticas Gerais, Livraria Escolar Editora, Lisboa, 1967.
- HALMOS, P. R., Naive Set Theory, D. Van Nostrand, Company, Inc., Princeton, New Jersey, 1960.
- OLIVEIRA, A. J. Franco de, Teoria dos Conjuntos Intuitiva e Axiomática (ZFC), Livraria Escolar Editora, Lisboa, 1982.
- SARRICO, C. S., Análise Matemática, Leituras e Exercícios, Gradiva, Lisboa, 1997.