Outro processo de sumir de (8) as coordenadas x e y consiste em relacioná-las com x' e y'. Exemplifico supondo

$$(9)\quad k\sqrt{\frac{a^2-e^2x'^2}{a^2-e^2x^2}}=n,\ \text{ou}\ n^2x'^2=k^2x^2+(n^2-k^2)\frac{a^2}{e^2}.$$

Das igualdades (6) se tiram $x'=(1-n)X+nx$, $y'=(1-n)Y+ny$, da primeira destas e de (9)

$$(10)\quad (n^4-k^2)x^2+2n^3(1-n)Xx+$$
$$+n^2(1-n)^2X^2-\frac{a^2}{e^2}(k^2-n^2)=0,$$

e de ambas

$$(11)\quad a^2Yy+b^2Xx=\frac{n-1}{2n}(a^2Y^2+b^2X^2)+\frac{n+1}{2n}a^2b^2.$$

Daqui, fazendo $\frac{n-1}{2n}(a^2Y^2+b^2X^2)+\frac{n+1}{2n}a^2b^2=Z$ sai a equação $b^2(a^2Y^2+b^2X^2)x^2-2b^2XZx+$ $+Z^2-a^4b^2Y^2=0$ e resultante dela e de (10) será uma equação do 8.º grau em qualquer das variáveis, que define a envolvida e evito desenvolver. Simplifico-a supondo $n^2=k$, o que permite deduzir de (10) a fórmula

$$Xx=\frac{n-1}{2n}X^2+\frac{n+1}{2n}\frac{a^2}{e^2}$$

e converte (11) em

$$b^2Y^2\left[a^2X^2-\left(\frac{n-1}{2n}X^2+\frac{n+1}{2n}\frac{a^2}{e^2}\right)^2\right]=$$
$$=a^2X^2\left[\frac{n-1}{2n}Y^2-\frac{n+1}{2n}\frac{1-e^2}{e^2}b^2\right]^2$$

que define uma curva do 6º e 4º grau, que é a envolvida. Duas tangentes a ela tiradas pelos extremos dum arco MN, cujas abcissas satisfazem à condição $x'^2=kx^2+(1-k)\frac{a^2}{e^2}$, intersectarão na elipse o arco $M'N'=k\cdot MN$.

4. Se a curva S for uma hipérbole, com o centro na origem das coordenadas e os semi-eixos a e b ao longo de abcissas e ordenadas, serão

$$b^2x^2-a^2y^2=a^2b^2=b^2x'^2-a^2y'^2,$$
$$\frac{a^2b^2+a^2yy'-b^2xx'}{ab(xy'-x'y)}=\frac{t}{\sqrt{e^2x^2-a^2}}=$$
$$=\frac{t'}{\sqrt{e^2x'^2-a^2}},\ a^2e^2=a^2+b^2,$$

mas sendo a sua equação a mesma da elipse com a simples mudança de b^2 em $-b^2$, mantém-se para a primeira cónica os resultados adquiridos para a segunda, uma vez feita tal mudança. É pois possível numa hipérbole marcar arcos cujos comprimentos tem um cociente constante, e por meio de operações algébricas.

5. Dado numa cónica centrada um arco PQ, tirem-se as tangentes pelos seus extremos até o ponto de cruzamento T, pelo qual se faça passar outra cónica confocal com a primeira: e marque-se nesta um arco $P'Q'$ tal que as tangentes pelos seu extremos se cruzem na segunda. Diz o teorema do Dr. Graves que é rectificável a diferença $PQ-P'Q'$, mas marcando na cónica um arco $P'M=PQ$, essa diferença converte-se em $P'M-P'Q'=Q'M$. Há pois numa cónica centrada uma série infinda de arcos rectificáveis; e na elipse ela é diferente da descoberta por Rodolfo Guimarães.

MATEMÁTICAS ELEMENTARES

Axiomática de Peano

Demonstração das propriedades da adição e multiplicação pelo método de indução

por *J. da Silva Paulo*

0. Introdução

Trata a Aritmética do estudo das propriedades dos números e a sua construção pode fazer-se de vários modos de acordo com a maneira como é introduzido o conceito de número, mas em todos eles ordenando devidamente as proposições que formam o corpo da teoria. Para essa ordenação deve ter-se em conta que no desenvolvimento duma teoria dedutiva, como é a Aritmética, o reconhecimento da verdade duma proposição, isto é a sua demonstração, se obtem como consequência lógica de outras, anteriormente reconhecidas verdadeiras. A demonstração faz-se assim à custa de todas ou parte das proposições que antecedem aquela cuja verdade se quer reconhecer, e, por isso, torna-se evidente que tem de existir uma ou mais

proposições iniciais que, por serem as primeiras, não poderão demonstrar-se.

Aceitam-se, então, sem demonstração certas proposições, inicialmente, as quais tomam o nome indiferentemente de *axiomas*, *postulados* ou *proposições primitivas* [1].

É bem claro que tais proposições terão de satisfazer às seguintes condições:

1.º). Serem *independentes*, isto é, nenhuma delas ser consequencia lógica de todas as outras, ou o que é a mesma coisa, não ser demonstravel a partir do conjunto das restantes.

2.º). Não serem *contraditórias*, isto é, delas não se poderem deduzir lógicamente duas proposições, que sejam a negação uma da outra.

3.º). Serem suficientes para a dedução de todas as propriedades, que se deseja estudar.

Procura-se ainda, em geral, que elas sejam as mais simples possível.

A sua introdução, para o desenvolvimento da teoria, ou se faz tomando-as todas em conjunto, de início, ou à medida que se torna necessário para a construção do edifício lógico.

Mas não bastam estas proposições. É necessário ainda a introdução de conceitos que delimitam o campo de aplicação da teoria e se referem aos entes a que ela é aplicável. Esta definição faz-se tambem à custa de conceitos ou ideias anteriormente definidos e teremos, por isso, que partir de certas *ideias primitivas*, que, do mesmo modo, não se definem.

Uma teoria assim construida e desenvolvida é o que se chama uma teoria axiomática.

O conjunto de propriedades que se escolhem como axiomas para uma dada teoria é um tanto arbitrário, e assim se nos apresentam várias axiomáticas para a mesma teoria.

Na teoria dos números, pode assim começar-se por uma teoria dos números *inteiros não negativos*, que depois se ampliará sucessivamente, à dos números inteiros, à dos racionais, à dos reais e finalmente à teoria dos números complexos.

[1] Euclides, ao axiomatizar a Geometria separou as proposições iniciais em dois grupos que denominou de axiomas e postulados. Aqueles não eram senão o conjunto de propriedades próprio para caracterizar as grandesas em geral, e estes, os postulados, as proposições referentes, mais especificamente, aos entes da geometria, se bem que nos *Elementos* nada se diga acerca do que são os axiomas e os postulados. Quiz-se, depois, justificar essa distinção dizendo-se que ela se baseava na maior ou menor evidencia das proposições, o que é de apreciação muito subjectiva e por isso insuficiente. Hoje, não se faz distinção alguma, usando-se, indiferentemente qualquer das designações citadas para aquele conjunto de proposições que se aceitam sem demonstração.

É este o metodo usado por Peano na sua teoria dos números e é êle que vamos seguir para a dedução das propriedades da adição e da multiplicação de números inteiros não negativos.

1. Axiomática de Peano

As ideias primitivas que se tomam na teoria dos números inteiros não negativos, de Peano, são as de:

$I_p 1$. Número inteiro [1].

$I_p 2$. Sucessor de um inteiro

$I_p 3$. Zero.

O significado destes conceitos será esclarecido com os axiomas da teoria.

Representaremos por N_0 o conjunto dos inteiros não negativos, os quais serão representados por letras minusculas $(a, b, c \cdots)$, e o zero por 0.

O sucessor de um inteiro a será representado por a^+.

O conjunto N_0 dos inteiros, bem como 0 e sucessor são então noções primitivas, que aceitamos sem definição como dados da experiência.

Entre os inteiros de N_0 existe uma relação, a que chamaremos de igualdade, simbólicamente representada por $=$, tal que dados dois inteiros quaisquer a e b duas hipóteses se podem verificar: ou a relação existe entre eles e escreveremos $a = b$ ou a relação não existe e escreveremos $a \neq b$. Esta relação é caracterizada pelas seguintes propriedades (axiomas):

Quaisquer que sejam a, b e c

$I 1$. $a = a$

$I 2$. Se $a = b$ então $b = a$

$I 3$. Se $a = b$ e $b = c$ então $a = c$.

As *proposições primitivas* da teoria são:

$P_p 1$. Zero é um número inteiro.

$P_p 2$. Todo o número inteiro a tem um único sucessor a^+ que é também um número inteiro.

$P_p 3$. Se a e b são números inteiros e $a^+ = b^+$, então $a = b$.

$P_p 4$. O sucessor de um número inteiro não pode ser zero.

$P_p 5$. (Princípio de indução finita) [2].

Se K é uma classe de inteiros que gosa das seguintes propriedades:

1.º). 0 pertence a K;

2.º). O facto de n pertencer a K implica (determina) que n^+ pertence tambem a K;

então a classe K contem todos os inteiros, isto é, coincide com N_0.

[1] Diremos muitas vezes número, número inteiro, ou inteiro por número inteiro não negativo.

[2] Existe um *principio de indução transfinita*.

O axioma $P_p 1$ diz-nos que o conjunto N_0 dos números inteiros não é vazio, pois contem pelo menos o zero.

O axioma $P_p 2$ afirma que o sucessor de um número é um número bem determinado, visto que ele é único, e podia enunciar-se sob a forma:

$$\text{Se } a = b \text{ então } a^+ = b^+.$$

Daqui se conclue que $a \neq a^+$, qualquer que seja a, pois se assim não fosse seria também $a^+ = (a^+)^+$ e a não teria um único sucessor.

O axioma $P_p 3$ afirma a unicidade do antecessor de um número dado, se chamarmos antecessor de a^+ ao número a.

$P_p 4$ pode enunciar-se sob outra forma: *Zero não é sucessor de algum número.* Ou então:

Se a é um número e $a = b^+$ então $a \neq 0$.

Veremos mais tarde que zero é o único elemento que não tem antecessor.

O axioma $P_p 5$ vai permitir a demonstração dum muito importante:

Teorema 1. (*Teorema de indução*). Se a uma proposição $P(x)$ se pode fazer corresponder um inteiro x de tal modo que:

1.º). Para $x=0$, $P(0)$ é verdadeira;

2.º). O facto de $P(n)$ ser verdadeira implica que $P(n^+)$ também é verdadeira;

então $P(x)$ é verdadeira para todos os inteiros de N_0.

Dem. Seja K a classe dos inteiros para os quais $P(x)$ é verdadeira. Pela hipótese do teorema tem-se:

1.º). 0 pertence a K, pois $P(0)$ é verdadeira;

2.º). Se n pertence a K então n^+ pertence também a K, pois que se $P(n)$ é verdadeira também $P(n^+)$ o é;

então K, pelo princípio de indução, contém todos os inteiros de N_0, isto é, $P(x)$ é verdadeira para todos os inteiros de N_0, c. q. d.

Este teorema fornece-nos um método de demonstração que sistemáticamente usaremos no que se segue.

A demonstração pelo *método de indução* consta então de duas partes:

1.º). Verifica-se ou demonstra-se que a proposição é verdadeira para o inteiro zero; e

2.º). Demonstra-se que se ela for verdadeira para o inteiro n o é também para o seu sucessor n^+.

Definição 1. Ao sucessor de 0 chamaremos 1 (um), isto é, $0^+ = 1$.

Poderiamos agora dar uma regra [1] para representação de todos os inteiros, mas para o estudo que faremos essa representação não interessa.

2. Adição

Definição 2. Se a, b e c forem números inteiros quaisquer chamaremos adição $(+)$ à operação que verifica as seguintes condições:

$A1.\ a + 0 = a;$

$A2.\ a + b^+ = (a + b)^+.$

Demonstraremos agora pelo método de indução o seguinte:

Teorema 2. Se a e b são inteiros então $a+b$ é um inteiro.

Dem. A proposição $P(x)$ é o enunciado do teorema, e o inteiro x que vamos fazer corresponder à proposição é o inteiro b.

Então verificaremas que:

1.º). Para $b=0$ a proposição é verdadeira. De facto para $b=0$ vem

$$a + 0 = a \quad \text{por } A1$$

e como a é um inteiro a proposição é verdadeira.

E demonstraremos que:

2.º). Se a proposição é verdadeira para o inteiro n ela também é verdadeira para o inteiro n^+.

Suponhamos então que

$$a + n \text{ é um inteiro}$$

como $a+n^+ = (a+n)^+$ por $A2$ e como o facto de $a+n$ ser inteiro implica que $(a+n)^+$ é um inteiro, por $P_p 2$, segue-se que $a + n^+$ é também um inteiro.

Então verificam-se as condições do teorema de indução, a saber:

A proposição pode fazer-se corresponder um inteiro b, e

1.º). A proposição é verdadeira para $b=0$;

2.º). O facto da proposição ser verdadeira para $b=n$ implica que ela é verdadeira para $b=n^+$; então

---

[1] A regra poderia ser a seguinte: os sucessores dos números seriam formados do seguinte modo: $0^+=1$, $1^+=2$, $2^+=3$, $3^+=4$, $4^+=5$, $5^+=6$, $6^+=7$, $7^+=8$, $8^+=9$, $9^+=10$, e daqui por diante do seguinte modo: o sucessor de um número em que o último algarismo da direita seja diferente de 9 é o número que se obtem substituindo êsse último algarismo pelo seu sucessor; se o último algarismo da direita for um 9, substitue-se este por 0 e o número, formado pelos restantes algarismos à esquerda do 9, pelo seu sucessor formado pela regra antecedente.

Algarismo chama-se a qualquer dos números

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9.$$

o teorema é verdadeiro qualquer que seja o inteiro b de N_0 que se adicione a outro inteiro a dado [1].

TEOREMA 3. (*Uniformidade*). Se $a=b$ então

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

Dem. Demonstraremos o teorema por indução em c. Então verificaremos que:

1.º). O teorema é verdadeiro para $c=0$. De facto

$$a + 0 = b + 0$$

o que implica, por $A1$, $I2$, $I3$: $a=b$, verdadeira por hipótese.

2.º). Se $a+n=b+n$ for verdadeira será

$$a + n^+ = (a + n)^+ \text{ por } A2$$

e

$$b + n^+ = (b + n)^+ \text{ por } A2 .$$

Ora de $a+n=b+n$ deduz-se por $P_p 2$ que

$$(a + n)^+ = (b + n)^+$$

e daqui e das igualdades anteriores, em vista de $I2$ e $I3$, que

$$a + n^+ = b + n^+ .$$

Finalmente pelo teorema de indução se conclue que o teorema 3 é verdadeiro qualquer que seja c de N_0.

TEOREMA 4. $0+a=a$.

Dem. Por indução em a.

1.º). Para $a=0$ vem

$$0 + 0 = 0 \text{ verdadeiro por } A1 .$$

2.º). Se $0+n=n$ for verdadeira será

$$0 + n^+ = (0 + n)^+ = n^+$$

e o teorema é verdadeiro qualquer que seja a, de N_0.

COROLÁRIO. De $A1$ e Teor. 4 resulta

$$a + 0 = 0 + a = a$$

TEOREMA 5. $a+1=a^+$.

Dem. Como $0^+=1$ (Def. 1) é

$$a + 1 = a + 0^+ = (a + 0)^+ = a^+ \text{ por } A1 \text{ e } P_p 2 .$$

TEOREMA 6. $1+a=a^+$.

Dem. Por indução em a.

1.º). Para $a=0$ vem

$$1 + 0 = 0^+$$

e de

$$0^+ = 1$$

resulta

$$1 + 0 = 1$$

e o teorema é verdadeiro por $A1$.

2.º). Se for $1+n=n^+$ verdadeiro será

$$1 + n^+ = (1 + n)^+ \text{ por } A2$$

e como de

$$1 + n = n^+$$

se deduz que

$$(1 + n)^+ = (n^+)^+ \text{ por } P_p 2 ,$$

será

$$1 + n^+ = (n^+)^+$$

e portanto o teorema é verdadeiro qualquer que seja a de N_0.

COROLÁRIO. Dos Teor. 5 e 6 deduz-se

$$a + 1 = 1 + a = a^+ \text{ [1]}$$

TEOREMA 7. $a+b^+=a^++b$.

Dem. Por indução em b.

1.º). Para $b=0$ vem

$a + 0^+ = (a + 0)^+ = a^+ = a^+ + 0$ e o teorema é verdadeiro.

2.º). Se for $a+n^+=a^++n$ verdadeira, será

$$a + (n^+)^+ = (a + n^+)^+ \text{ por } A2$$
$$a + (n^+)^+ = (a^+ + n)^+ \text{ por hipótese}$$
$$a + (n^+)^+ = a^+ + n^+ \text{ por } A2$$

o que conclue a demonstração.

TEOREMA 8. (*Comutatividade*). $a+b=b+a$.

Dem. Por indução em b.

1.º). Para $b=0$ temos

$$a + 0 = 0 + a$$

verdadeiro pelo corolário do Teor. 4.

2.º). Se for $a+n=n+a$ será

$$a + n^+ = (a + n)^+ = (n + a)^+ = n + a^+$$

e como pelo teorema 7 é $n+a^+ = n^++a$ vem

$$a + n^+ = n^+ + a$$

o que conclui a demonstração.

---

[1] De algum modo se pode dizer que o teorema sendo verdadeiro para 0 é verdadeiro para 1, porque sendo verdadeiro para um inteiro é verdadeiro para o seguinte, e sendo verdadeiro para 1 é também verdadeiro para 2 e assim por diante para todos os inteiros. No fundo é este mecanismo que justifica o método.

[1] Os Teor. 5 e 6 justificam a regra que demos em nota para a representação dos inteiros, pondo-a de acordo com os conhecimentos e intuições do aluno.

TEOREMA 9. (*Associatividade*). $(a+b)+c=a+(b+c)$

Dem. Por indução em c.

1.º). Para $c=0$ vem

$$(a+b)+0=a+b$$

e

$$a+(b+0)=a+b$$

donde

$$(a+b)+0=a+(b+0)$$

e o teorema é verdadeiro.

2.º). Se for $(a+b)+n=a+(b+n)$ verdadeira será:

$$(a+b)+n^+=[(a+b)+n]^+=[a+(b+n)]^+=a+(b+n)^+$$

$$(a+b)+n^+=a+(b+n^+) \qquad \text{c. q. d.}$$

TEOREMA 10. (*Lei do Corte ou da Simplificação*). Se $a+c=b+c$ então $a=b$.

Dem. Por indução em c.

1.º). Para $c=0$ vem

$$a+0=b+0 \text{ implica } a=b$$

e o teorema é verdadeiro;

2.º). Se de $a+n=b+n$ se deduz $a=b$, então de

$$a+n^+=b+n^+$$

ou de

$$(a+n)^+=(b+n)^+$$

deduz-se

$$a+n=b+n \text{ por } P_p 3,$$

e daqui pela hipótese

$$a=b. \qquad \text{c. q. d.}$$

COROLÁRIO. Em vista do teorema 8 também

$$c+a=c+b \text{ implica } a=b.$$

TEOREMA 11. O zero é único, isto é, só existe um inteiro para o qual é

$$a+0=a$$

qualquer que seja a.

Dem. Suponhamos que existia outro inteiro u tal que $a+u=a$ qualquer que fosse a. Então seria por *I*2 e *I*3

$$a+u=a+0$$

e pelo teorema 10

$$u=0$$

qualquer que seja a.

TEOREMA 12. Se $a\neq 0$ então existe um inteiro b tal que $a=b^+$.

Dem. Como o zero é único, se a não fosse sucessor de algum inteiro seria, por $P_p 4$, (definição do zero) o próprio zero, o que é contrário à hipótese $a\neq 0$.

TEOREMA 13. Se $a\neq 0$ então $a+b\neq 0$.

Dem. Por indução em b.

1.º). Para $b=0$ vem

$$a+0\neq 0$$

por hipótese e o teorema é verdadeiro.

2.º). Se for $a+n\neq 0$ verdadeiro então $a+n^+=(a+n)^+$ é diferente de 0 porque o sucessor de um inteiro não pode ser zero, isto é,

$$a+n^+\neq 0$$

o que conclui a demonstração.

TEOREMA 14. Se $a+b=0$ então $a=0$ e $b=0$.

Dem. É $a=0$, porque se fosse $a\neq 0$ pelo teorema 13 era $a+b\neq 0$.

Então vem

$$a+b=0+b=0$$

e

$$b=0$$

TEOREMA 15. Se a equação $a+x=b$ tiver uma solução esta é única.

Dem. De facto, se houvesse outra y seria $a+y=b$ e por *I*2 e *I*3

$$a+x=a+y \quad .$$

donde

$$x=y.$$

DEFINIÇÃO 3. Se houver um inteiro $x\neq 0$ tal que

$$a+x=b$$

diremos que b é maior que a. Simbòlicamente $b>a$. Com o mesmo significado escreveremos $a<b$ que se lê a menor que b.

TEOREMA 16. $a^+>a$

Dem. Como $a^+=a+1$ e $1\neq 0$, pela Definição 3 vem

$$a^+>a.$$

De $a^+=a+1$ deduz-se ainda se for $a\neq 0$ que $a^+>1$.

TEOREMA 17. Se $a\neq 0$ então $a>0$.

Dem. De facto se $a\neq 0$ como $a=0+a$ pela Def. 3 é

$$a>0.$$

O teorema pode ainda enunciar-se:

Zero é o menor de todos os números inteiros.

TEOREMA 18. Se $a>b$ e $b>c$ então $a>c$.

Dem. Se $a>b$ e $b>c$ então será

$$a = b + x \quad \text{e} \quad b = c + y \quad \text{com } x \neq 0 \text{ e } y \neq 0$$

logo

$$a = b + x = (c + y) + x = c + (y + x)$$

e como $x + y \neq 0$ (Teor. 13) é

$$a > c .$$

TEOREMA 19. Se $a>b$ então $a^+>b^+$.

Dem. Se $a>b$ então é $a=b+x$ com $x\neq 0$ e portanto $a^+=(b+x)^+$ com $x\neq 0$ ou

$$a^+ = b + x^+ = b^+ + x \quad \text{com} \quad x \neq 0$$

e portanto

$$a^+ > b^+ .$$

TEOREMA 20. Se $a^+>b^+$ então $a>b$.

Dem. Se $a^+>b^+$ então é $a^+=b^++x=x+b^+$ com $x\neq 0$ ou $a^+=(x+b)^+$ e portanto

$$a = x + b \text{ com } x \neq 0 \text{ e } a > b .$$

TEOREMA 21. Se $a>b$ então $a+c>b+c$.

Dem. Por indução em c.

1.º). Para $c=0$ vem

Se $a>b$ então $a+0>b+0$ e o teorema é verificado.

2.º). Se de $a>b$ se conclue que $a+n>b+n$ então de $a>b$ conclue-se que

$$(a + c)^+ > (b + c)^+$$

por Teor. 19 ou seja de $a>b$ conclue-se que

$$a + c^+ > b + c^+$$

e o teorema é verdadeiro para qualquer c de N_0.

TEOREMA 22. Se $a+c>b+c$ então $a>b$.

Dem. Por indução em c.

Análoga à anterior.

DEFINIÇÃO 4. Se houver um inteiro x qualquer tal que

$$a + x = b$$

diremos que b é *maior ou quando muito igual a* a. Simbólicamente $b\geqslant a$. Com o mesmo significado escreveremos $a\leqslant b$ que se lê *a menor ou quando muito igual a* b.

Observe-se que se $x=0$ então $a=b$ e se $x\neq 0$, pelo Teor. 3, $a>b$. Então $a\leqslant b$ significará também que *ou* $a=b$ *ou* $a<b$.

TEOREMA 23. Se $a\neq 0$ então $a\geqslant 1$.

Dem. Como $a\neq 0$ então pelo teor. 12 é $a=b^+=b+1$ e pela def. 4 $a\geqslant 1$.

TEOREMA 24. Se $a\geqslant b$ e $b\geqslant a$ então $a=b$.

Dem. Se $a\geqslant b$ então $a=b+x$ e se $b\geqslant a$ então $b=a+y$ de modo que é

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

ou ainda

$$a + 0 = a + (y + x)$$

donde se conclue por Teor. 10 ser

$$y + x = 0 \quad \text{e pelo Teor. 14}$$
$$y = x = 0 .$$

Finalmente obtem-se

$$a = b + 0 = b$$

TEOREMA 25. Se $a\geqslant b$ e $b\geqslant c$ então $a\geqslant c$.

Dem. Se $a\geqslant b$ e $b\geqslant c$ é $a=b+x$ e $b=c+y$ donde $a=(c+y)+x=c+(x+y)$ e portanto

$$a \geqslant c .$$

TEOREMA 26. Se $a=b$ e $b>c$ então $a>c$.

Dem. Se $b>c$ então é $b=c+x$, $x\neq 0$, logo $a=c+x$ e portanto $a>c$.

TEOREMA 27. Se $a=b$ e $b\geqslant c$ então é $a\geqslant c$.

Dem. Análoga à anterior.

TEOREMA 28. Dados dois inteiros quaisquer a e b, entre eles existe uma e uma só das seguintes relações

$$a > b$$
$$a = b$$
$$a < b$$

Dem. por indução em b.

1.º). Para $b=0$ vem

se $a=0$ $a=b$

se $a\neq 0$ então $a>b$ pelo teorema 17 e o teorema é verdadeiro.

2.º). Se para $b=n$ uma e uma só das relações

$$a > n$$
$$a = n$$
$$a < n$$

se verifica, então para $b=n^+$ vem

A). Se $a>n$ então $a=n+x$ com $x\neq 0$ ou seja $x\geqslant 1$ (teor. 18) ou ainda $x=1+y$ e daqui resulta

$$a = n + (1 + y) = (n + 1) + y = n^+ + y$$

donde

$$a \geqslant n^+$$

quer dizer: se $a>n$ então ou

$$a > n^+ \quad \text{ou} \quad a = n^+ .$$

B). Se $a=n$ então $n^+=n+1=a+1$ e $a<n^+$.

C). Se $a<n$ então $n=a+x$, $x\neq 0$, donde $n^+ = (a+x)^+ = a+x^+$ e portanto

$$a<n^+.$$

E o teorema é verdadeiro qualquer que seja b de N_0.

DEFINIÇÃO 5. Diremos que a está entre b e c ($b<c$) quando for $b<a$ e $a<c$, ou abreviadamente $b<a<c$.

TEOREMA 27*. Entre 0 e 1 não existe qualquer inteiro.

Dem. Se existisse a tal que $0<a<1$ então seria $a\neq 0$ pelo Teor. 28, e pelo Teor. 23 era $a\geqslant 1$ o que é incompatível com a hipótese $a<1$. Logo não pode existir um inteiro a entre 0 e 1.

EXERCÍCIOS:

Demonstrar que:

1). $a\not> a$ (a não é maior que a);
2). $a\geqslant 0$;
3). $a\geqslant a$;
4). Se $a>b$ e $c>d$ então $a+c>b+d$ (sugestão: empregue $a>b$ e $c=c$ e depois $b=b$ e $c>d$);
5). Se $b\geqslant a$ então $b+c\geqslant a+c$;
6). Se $b\geqslant a$ e $d\geqslant c$ então $b+d\geqslant a+c$.

3. Multiplicação

DEFINIÇÃO 2'. Se a, b, e c forem números inteiros quaisquer, chamaremos multiplicação ($\times$) à operação que verifica as seguintes condições:

$$M1.\quad a\times 0 = 0$$
$$M2.\quad a\times b^+ = a\times b + a\ ^{(1)}.$$

TEOREMA 2'. Se a e b são inteiros então $a\times b$ é um inteiro.

Dem. Por indução em b.
1.º). Para $b=0$ vem

$$a\times 0 = 0 \text{ por } M1$$

e o teorema é verificado.
2.º). Se for $a\times n$ um inteiro então

$$a\times n^+ = a\cdot n + a$$

é um inteiro visto $a\cdot n$ e a serem inteiros e em virtude ainda do teor. 2.

O teorema é então verdadeiro pelo teorema de indução.

(1) Em vez do sinal $\times$ usaremos algumas vezes o sinal $\cdot$ ou escreveremos mesmo ab por $a\times b$ ou $a\cdot b$

Observemos desde já que existe um absoluto paralelismo entre as propriedades da adição e as da multiplicação. Esse paralelismo pode ser aproveitado para evitar muitas demonstrações, desde que a axiomática usada para definir as duas operações seja análoga. Ora não é o caso presente como se verifica comparando os axiomas $A1$, $A2$ e $M1$, $M2$. Em alguns casos as demonstrações de propriedades idênticas da adição e da multiplicação são semelhantes, mas é fácil verificar que não o são em absoluto pela causa apontada. E desde que as definições de adição e multiplicação sejam as de Grassman, que adoptamos, e o método de demonstração o de indução, em geral, é impossivel decalcar as demonstrações das propriedades da multiplicação a partir das da adição ou vice-versa, ainda pela razão da falta de simetria entre as fórmulas $A1$, $A2$ e $M1$, $M2$; isto, mesmo que a adição se definisse em N_0 e a multiplicação em N_1 (1).

TEOREMA 3'. (*Uniformidade*). Se $a=b$ então

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

Dem. Por indução em c.
1.º). Para $c=0$ vem

$$a\cdot 0 = b\cdot 0$$

e o teorema é verificado em vista de $M1$.
2.º). Se de $a=b$ se puder deduzir $a\times n=b\times n$ então desta última deduz-se

$$a\cdot n + a = b\,.\,n + b \qquad \text{pelo Teor. 3}$$

ou

$$an^+ = bn^+$$

portanto

$$\text{se } a=b \text{ então } a\cdot n^+ = b\cdot n^+$$

e o teorema é verdadeiro.

TEOREMA 28. $0\,.\,a=0$.

Dem. Por indução em a.
1.º). Para $a=0$ vem

$$0\,.\,0 = 0 \text{ por } M1$$

e o teorema é verificado;
2.º). Se for $0\,.\,n=0$ então

$$0\,.\,n^+ = 0\,.\,n + 0 = 0 \qquad \text{c. q. d.}$$

COROLÁRIO. De $M1$ e Teor. 28 conclue-se que

$$a\,.\,0 = 0\,.\,a = 0.$$

TEOREMA 29. $a.\,1=a$.

Dem. Como $0^+=1$ substituindo em $M2$ vem

$$a\,.\,0^+ = a\,.\,0 + a$$

ou

$$a\,.\,1 = a$$

(1) Costuma representar-se por N o conjunto dos números inteiros positivos.

TEOREMA 4'. $1 . a = a$.

Dem. Por indução em a.
1.º). Para $a=0$ vem

$$1 . 0 = 0 \text{ verdadeiro por } M1;$$

2.º). Se $1 . n = n$ for verdadeira será

$$1 . n^+ = 1 . n + 1 = n + 1 = n^+$$

e o teorema é verdadeiro.

COROLÁRIO. De Teor. 29 e Teor. 5' conclui-se que $a . 1 = 1 . a = a$.

TEOREMA 30. $b^+ . a = b . a + a$.

Dem. Por indução em a.
1.º). Para $a=0$ vem

$$b^+ . 0 = b . 0 + 0$$
$$0 = 0$$

e o teorema é verificado;
2.º). Se for $b^+ . n = b . n + n$ então

$$b^+ . n^+ = b^+ n + b^+ = (bn + n) + b^+ = bn + (n + b^+) =$$
$$= bn + (n + b)^+ = [bn + (n + b)]^+ = [bn + (b + n)]^+ =$$
$$= [(bn + b) + n]^+ = (bn^+ + n)^+ = bn^+ + n^+$$

isto é

$$b^+ . n^+ = bn^+ + n^+$$

e o teorema é verdadeiro.

TEOREMA 31. *(Distributividade).* $a . (b+c) = ab + ac$.

Dem. Por indução em c.
1.º). Para $c=0$ vem

$$a . (b + 0) = ab + a . 0$$

ou

$$ab = ab$$

e o teorema é verificado;
2.º). Se for $a . (b+n) = ab + an$ então

$$a . (b+n^+) = a . (b + n)^+ = a . (b + n) + a =$$
$$= (ab + an) + a = ab + (an + a) = ab + an^+$$

isto é

$$a . (b + n^+) = ab + an^+ \qquad \text{c. q. d.}$$

TEOREMA 8'. *(Comutatividade).* $a . b = b . a$.

Dem. Por indução em b.
1.º). Para $b=0$ vem

$$a . 0 = 0 . a$$

que pelo Corolário do Teor. 28 é verdadeira, e o teorema é verificado;
2.º). Se for $a . n = n . a$ então

$$a . n^+ = an + a \text{ por } M2$$
$$= na + a$$
$$= n^+ . a \text{ pelo Teor. 30.}$$

TEOREMA 9'. *(Associatividade).* $(a . b) . c = a . (b . c)$.

Dem. Por indução em c.
1.º). Para $c=0$ vem

$$(a . b) . 0 = a . (b . 0)$$
$$0 = a . 0$$

e o teorema é verificado;
2.º). Se for $(a . b) . n = a . (b . n)$ então

$$(a . b) . n^+ = (a . b) . n + ab = a . (b . n) + ab =$$
$$= a . [(b . n) + b] = a . (b . n^+)$$

isto é

$$(a . b) . n^+ = a . (b . n^+)$$

e o teorema é verdadeiro qualquer que seja c de N_0.

TEOREMA 10'. *(Lei do corte ou da simplificação).* Se $a . b = a . c$ e $a \neq 0$ então $b = c$.

Dem. Como $a \neq 0$ será $a = d^+$ pelo Teor. 12.
O enunciado do teorema é então equivalente ao seguinte: «Se $d^+ . b = d^+ . c$ então $b = c$».

Dem. Por indução em d.
1.º). Para $d=0$ vem

de $0^+ . b = 0^+ . c$ deduz-se $1 . b = 1 . c$ ou $b = c$

e o teorema é verificado;
2.º). Se, de $n^+ . b = n^+ . c$ se deduz que $b = c$, então será: de $(n^+)^+ . b = (n^+)^+ . c$ deduz-se $n^+ . b + b = n^+ . c + c$ pelo Teor. 30 e daqui por ser $n^+ . b = n^+ . c$ que $n^+ . b + b = n^+ . b + c$ e ainda pelo Teor. 10

$$b = c .$$

Quer dizer que de $(n^+)^+ . b = (n^+)^+ . c$ se deduz $b = c$ então o teorema é verdadeiro para qualquer $a \neq 0$.

COROLÁRIO. Em vista do Teor. 8' também de $b . a = c . a$ e $a \neq 0$ se deduz $b = c$.

TEOREMA 32. Se $a \neq 0$ e $b \neq 0$ então $ab \neq 0$.

Dem. Se $a \neq 0$ e $b \neq 0$ então $a = c^+$ e $b = d^+$ e teremos

$$c^+ . d^+ = c^+ . d + c^+$$

e como $c^+ \neq 0$ então, pelo Teor. 13,

$$a . b = c^+ . d + c^+ \neq 0 .$$

TEOREMA 33. Se $ab = 0$ e $a \neq 0$ então $b = 0$

Dem. Se $a \neq 0$ então $a = c^+$ e portanto

$$ab = c^+ . b = cb + b = 0$$

e pelo Teor. 14 é $cb = 0$ e $b = 0$.

TEOREMA 34. Se $ab=0$ então ou $a=0$ ou $b=0$.

Dem. Se for $a=0$ é $ab=0$ qualquer que seja b, pelo Teor. 28.

Se for $a\neq 0$ então é $b=0$ pelo Teor. 33.

Das duas hipóteses decorre a tese do teorema.

TEOREMA 35. Se $ab\neq 0$ então $a\neq 0$ e $b\neq 0$.

Dem. De facto a e b têm que ser ambos diferentes de zero porque se um qualquer deles fosse igual a zero então por $M1$ e Teor. 28 seria $ab=0$.

TEOREMA 14' Se $ab=1$ então $a=1$ e $b=1$.

Dem. Como $ab=1\neq 0$ será, pelo Teor. 35 $a\neq 0$ e $b\neq 0$; logo é $a=c^+$ e $b=d^+$, e então

$$ab = c^+ d^+ = c^+ d + c^+ = 1$$

ou seja

$$(c^+ d + c)^+ = 1$$

e por ser $0^+=1$, e o sucessor de um número ser único, vem

$$c^+ d + c = 0;$$

finalmente pelo Teor. 14

$$c^+ d = 0 \text{ e } c = 0$$

ou

$$0^+ d = 0 \text{ e } c = 0$$

$$\text{d} = 0 \text{ e } c = 0$$

e portanto

$$a = c^+ = 1$$

$$b = d^+ = 1$$

TEOREMA 15'. Se a equação $ax=b$, onde $a\neq 0$, tiver uma solução esta é única.

Dem. Se a equação tivesse outra solução y seria

$$a \,.\, y = b$$

e portanto

$$ax = ay$$

donde, por Teor. 10', pois $a\neq 0$

$$x = y$$

TEOREMA 21'. Se $b>c$ e $a\neq 0$ então $ba>ca$.

Dem. Como $a\neq 0$ então é $a=d^+$. Daqui o enunciado equivalente:

«Se $b>c$ e $a=d^+$ então $bd^+>cd^+$».

Dem. Por indução em d.

1.º). Para $d=0$ vem

de $b>c$ resulta $b\,.\,1>c\,.\,1$ ou seja $b\,.\,0^+>c\,.\,0^+$

e o teorema é verificado.

2.º). Se de $b>c$ resulta $b\,.\,n^+>c\,.\,n^+$ então de $b>c$ resulta também, Ex. 4, pág. 21,

$$bn^+ + b > cn^+ + c$$

donde

$$b\,(n^+)^+ > c\,(n^+)^+$$

quer dizer de

$$b>c \text{ resulta } b\,(n^+)^+ > c\,(n^+)^+$$

e o teorema é verdadeiro qualquer que seja $a\neq 0$.

COROLÁRIO. Pelo Teor. 8' é também:

Se $a\neq 0$ e $b>c$ então $ab>ac$.

TEOREMA 22'. Se $a\neq 0$ e $ba>ca$ então $b>c$.

Dem. Como $a\neq 0$ é $a=d^+$, e demonstraremos o teorema por indução em d.

1.º). Para $d=0$ vem

de $b\,.\,0^+>c\,.\,0^+$ deduz-se $b\,.\,1>c\,.\,1$ ou $b>c$

e o teorema é verificado;

2.º). Se, de $b\,.\,d^+>c\,.\,d^+$ se deduz $b>c$, também de

(A) $bd^+ + b > cd^+ + b$ se deduz $b>c$

porque de

$bd^+ > cd^+$ se deduz $bd^+ + b > cd^+ + b$.

Por outro lado

(B) de $cd^+ + b > cd^+ + c$ deduz-se $b>c$

pelo Teor. 22.

Então de (A) e (B) deduz-se $b>c$.

Quer dizer de

$$ba^+ + b > cd^+ + b \text{ e } cd^+ + b > cd^+ + c$$

ou seja de

$$bd^+ + b > cd^+ + c \text{ deduz-se } b>c$$

e finalmente de:

$$b\,.\,(d^+)^+ > c\,.\,(d^+)^+ \text{ deduz-se } b>c$$

então o teorema é verdadeiro para qualquer $a\neq 0$.

Esta demonstração podia fazer-se mais simplesmente por processo análogo à do Teor. 21'.

EXERCÍCIOS:

Demonstrar:

1). Se $a\geqslant b$ e $c\geqslant d$ então $ac\geqslant bd$;
2). Se $a>b$ e $c>d$ então $ac>bd$;
3). Se $a=b\neq 0$ e $c>d$ então $ac>bd$;
4). Se $a\neq 0$ e $c\geqslant d$ então $ac\geqslant ad$;
5). Se $ac\geqslant bc$ e $c\neq 0$ então $a\geqslant b$.

4. Subtracção e Divisão

A partir dos Teors. 15 e 15′ é fácil fazer o estudo paralelo das propriedades da Subtracção e da Divisão, se definirmos a Subtracção em N_0 e a Divisão em N_1. Quer dizer, vamos definir a Subtracção para todos os inteiros não negativos e a Divisão para os inteiros positivos, pois a classe N_0 tem todos os elementos de N_1 mais o zero.

DEFINIÇÃO 6. Dados a e b de N_0, se existir um número x de N_0 tal que

$$a = b + x$$

diremos que x é *a diferença entre a e b* e escreveremos

$$x = a - b$$

que se lê x igual a a menos b.

DEFINIÇÃO 6′. Dados a e b de N_1, se existir um número x de N_1 tal que

$$a = b \,.\, x$$

diremos que x é o cociente de a *por* b e escreveremos

$$x = a : b$$

que se lê x igual a a dividido por b.

Destas definições concluem-se logo algumas propriedades destas operações, assim:

TEOREMA 36. $b + (a - b) = a$

basta notar que

$$x = a - b \,.$$

TEOREMA 37. $a - a = 0$

Dem. Como $a = a + 0$ por $A1$, resulta da Def. 6 a tese.

TEOREMA 36′. $b \times (a : b) = a$

basta notar que

$$x = a : b \,.$$

TEOREMA 37′. $a : a = 1$

Dem. Como $a = a \,.\, 1$ pelo Teor. 29, resulta da Def. 6′ a tese.

Outras propriedades relacionadas com a ordem se podiam deduzir imediatamente, entre as quais, por exemplo, a seguinte:

$$\text{Se } a < b \text{ e } a > x \text{ então } a - x < b - x \,.$$

A condição para que exista x no caso da Subtracção é dada pela Def. 4, isto é, existirá a diferença $a - b$ quando for $a > b$.

Quanto à condição de existência do cociente no caso da Divisão, só se pode considerar depois do estudo da divisibilidade. Note-se porém que a relação $a \prec b$ (leia-se a divide b) define-se paralelamente à relação $a \leqslant b$, sendo a primeira definida em N_1 e a segunda em N_0. As propriedades das duas relações são análogas e o seu estudo pode fazer-se paralelamente.

Cabe aqui para terminar a demonstração dos seguintes teoremas:

TEOREMA 38. $a^+ - a = 1$.

Dem. Como $a^+ = a + 1$ pela Def. 6 vem a tese.

TEOREMA 39. Entre a e a^+ não existe qualquer inteiro.

Dem. Suponhamos que existia um inteiro x tal que $a < x < a^+$; daqui se deduz que

$$a - a < x - a < a^+ - a$$

ou

$$0 < x - a < 1$$

e como existe o inteiro $x - a$ por ser $x > a$, conclui-se que, se entre a e a^+ existisse um inteiro, então também entre 0 e 1 existiria um inteiro, o que é impossível pelo Teor. 27*.

Nota

A independência dos axiomas duma teoria pode mostrar-se do seguinte modo: constrói-se um sistema de elementos de natureza qualquer que verifiquem todos os axiomas com excepção de um.

Tal construção prova que aquele axioma, que não é válido para os elementos do sistema, é independente dos restantes axiomas que são verificados por tais elementos.

Mostremos por este processo a independência dos axiomas da igualdade: $I1$, $I2$ e $I3$. Para isso consideremos:

1.º). O sistema N_1 de todos os inteiros positivos e consideremos definida entre eles a relação «divide». Como se sabe diz-se que «a divide b» (simbòlicamente $a \prec b$) quando existe um inteiro x tal que $b = a \,.\, x$. Então para cada par ordenado de inteiros a e b, ou *a divide b* ou *a não divide b*.

Esta relação gosa das seguintes propriedades:

1). $a \prec a$ qualquer que seja a;

2). Se $a \prec b$ e $b \prec c$ então $a \prec c$;

e não gosa da propriedade simétrica, isto é, em geral

«Se a divide b, b não divide a».

Assim, neste sistema, a relação «divide», definida para cada par de elementos de N_1, mostra que $I2$ é independente de $I1$ e $I3$.

2.º). Consideremos ainda o sistema N_1 de todos os inteiros positivos e entre os seus elementos definida a relação seguinte:

«Diremos que dois inteiros a e b estão em relação se e só se $|a - b| \geq 0$ e $|a - b| < 3$ [1].

[1] O simbolo $|a - b|$ tem o significado de módulo do $(a - b)$ isto é, $a - b$ se $a \geq b$ e $b - a$ no caso contrário.

Quando a estiver em relação com b escreveremos $a \mathcal{R} b$. Também aqui para cada par ordenado de elementos a e b, *ou a está em relação com b, ou a não está em relação com b*.

Esta relação gosa das propriedades:

1). $a \mathcal{R} a$ pois que $|a-a|=0$;

2). Se $a \mathcal{R} b$ então $b \mathcal{R} a$, pois que $|a-b|=|b-a|$;

e não gosa, em geral, da propriedade transitiva, pois que «se $a \mathcal{R} b$ sendo $|a-b|=2$ e $b \mathcal{R} c$ sendo $|b-c|=2$ e além disso $a \neq c$ então a não está em relação com c porque $|a-c|=4>3$».

Este exemplo mostra a independência de $I3$.

3.º). Consideremos finalmente o sistema de todos os números primos

$$2,\ 3,\ 5,\ 7,\ 11\ldots$$

e entre os elementos do sistema definida a seguinte relação:

«Dois números primos a e b estarão em relação e escreveremos $a \mathrm{R} b$, se e só se a e b forem simultâneamente impares».

Assim dado um par ordenado de elementos a e b, ou *a está em relação com b* ou *a não está em relação com b*.

Esta relação gosa das seguintes propriedades:

1). Se $a \mathrm{R} b$ então $b \mathrm{R} a$, pois que se a e b são primos impares b e a são primos impares;

2). Se $a \mathrm{R} b$ e $b \mathrm{R} c$ então $a \mathrm{R} c$, por uma razão análoga à anterior;

e não gosa da propriedade reflexiva em geral, porque

«2 não está em relação com 2».

Fica assim demonstrado que $I1$ é independente de $I2$ e $I3$.

Os três sistemas e as relações aí definidas mostram então que no sistema de axiomas, que tomamos para caracterizar a relação de igualdade, estes são independentes.

Exemplos de sistemas que provam a independência dos Axiomas P_p1-P_p5, de Peano, podem ver-se em *Formulário Matemático*, 2.º volume, de Peano.

O método dos coeficientes indeterminados

por **Laureano Barros**

1. Os actuais programas do Ensino Liceal incluem alguns assuntos que ou não são tratados ou são muito mal tratados nos livros até há pouco adoptados. Pareceu-nos, portanto, que poderia ter interesse a publicação de um estudo correcto de alguns destes assuntos. E assim, julgamos de particular importância a consideração de certos pontos dos programas de Álgebra (6.º e 7.º anos) onde as ampliações a programas anteriores mais se fizeram sentir.

Nesta ordem de ideias, começaremos por fazer uma referência breve ao método dos coeficientes indeterminados, ou, mais particularmente, aos teoremas em que esse método se fundamenta.

A brevidade desta referência justifica-se pelo facto deste mesmo assunto já ter sido tratado nas páginas da *Gazeta de Matemática*: o n.º 22 publica, efectivamente, um artigo do colaborador J. J. Rodrigues dos Santos, intitulado «Estudo de algumas propriedades dos polinómios inteiros», para o qual chamamos a atenção do leitor. Neste artigo, a par daquelas propriedades elementares dos polinómios que, actualmente, também são referidas nos novos programas, trata-se com particular detalhe do método dos coeficientes indeterminados. Como se justifica então esta nossa nota? É que no teorema-base do método há, naquele artigo, um erro grave de demonstração (Nota 1) Por outro lado, o facto mais recente de em alguns cursos liceais ser repetido esse erro e em alguns outros se usar uma forma ainda mais grosseira para tratar a questão, tudo isto decidiu-nos à publicação desta nota.

Aproveitamos a oportunidade para acrescentar aos exercícios propostos por Rodrigues dos Santos, no já referido n.º 22 da *Gazeta*, alguns outros, igualmente simples, mas que poderão ter algum interesse para os estudantes que pretendem submeter-se ao exame do 3.º ciclo.

2. Como é sabido, um *polinómio de grau n* em x é do tipo $f_n(x)=a_0x^n+a_1x^{n-1}+a_2x^{n-2}+\cdots+a_{n-1}x+a_n$, onde $a_0, a_1, a_2, \cdots a_n$ são os coeficientes. O valor de um polinómio $f_n(x)$ para $x=\alpha$ representa-se por $f_n(\alpha)$. Diz-se que um α é um *zero* ou *raiz* de $f_n(x)$ quando $f_n(\alpha)=0$.

Um polinómio $f_n(x)$ é *identicamente nulo*, quando é nulo para todos os valores de x; por outras palavras, um polinómio idênticamente nulo é o que admite para zero *qualquer* número real. Escreve-se $f_n(x)\equiv 0$.

Teorema fundamental. *Se $f_n(x)$ é identicamente nulo, são nulos todos os seus coeficientes.*