Prof. Dr. Abel Andrade, (100$00); Dr. Albuquerque Rodrigues, (200$00); Alexandre Sequeira, (1.000$00); Dr. António Breda, (200$00); António da Costa, (5.000$00); Dr. António Pais Rovisco, (200$00); Dr. Armando Gonçalves Pereira, (200$00); Dr. A. Palma Carlos, (300$00); Dr. Artur Brandão, (500$00); Dr. Augusto Soares, (1.000$00); A. Viana da Mota, (100$00); Banco Burnay, (4.000$00); Banco Espírito Santo e Com., (2.000$00); Banco Fonsecas, Santos e Viana, (5.000$00); Banco Português do Atlântico, (1.000$00); Dr. Bastos Guerra, (200$00); Benigno Delgado, (150$00); Eng.º Carlos Garcia Alves, (1.500$00); Carlos de Oliveira, (1.000$00); Companhia dos Diamantes de Angola, (10.000$00); Cónego Dr. Carneiro de Mesquita, (100$00); Crispim Rocha, (500$00); Estoril Plage, (1.000$00); F. Fernandes Guimarães, (500$00); Fernando Tavares de Carvalho, (500$00); F. Rocha Gonçalves, (1.000$00); Gabriel Ferreira Marques, (500$00); H. Vaultier & C.ª, (1.000$00); Dr. Hipólito Raposo, (300$00); J. Abreu Valente, (300$00); Dr. J. Azeredo Perdigão, (200$00); Dr. João Lourenço Castelo Branco, (200$00); Eng.º João Teixeira de Queiroz, (500$00); Dr. João Vieira de Araújo, (500$00); José Maria Pedroso e Neto, (500$00); José dos Santos Lima, (500$00); Dr. Lopes Fidalgo, (100$00); Luís Leal, (500$00); Prof. Dr. Manuel A. Moreira J.or, (500$00); Dr. Manuel Coelho, (200$00); Manuel Pimentel Cavalheiro, (50$00); Marcelino Nunes Correia, (1.000$00); Dr. Mário Calisto, (100$00); Dr. M. Colares Pereira, (300$00); Dr. Octávio de Brito, (500$00); Prof. Dr. Paulo da Cunha, (300$00); Dr. Pedro Chaves, (200$00); Sacor, (2.500$00); Sociedade Argibay de Construções Navais, Lda., (1.500$00); Sociedade Nacional dos Fósforos, (500$00); Dr. Tomaz Sanches da Gama, (1.000$00). Total 51.000$00.

Agôsto de 1944.

A «Dotação da J. I. M.» dispõe ainda de cotizações mensais e anuais que somavam, até Julho de 1944, 16.500$00 escudos.

A «Gazeta de Matemática» regista o êxito dêste empreendimento e salienta a circunstância de os subsídios concedidos definirem um princípio de colaboração entre entidades privadas e institutos científicos para-universitários, colaboração que a acentuar-se abriria animadoras perspectivas quanto à possibilidade da realização completa do programa da Junta de Investigação Matemática.

Pequena introdução à Álgebra Moderna — I.

por **J. Sebastião e Silva** (bolseiro em Roma do I. A. C.)

A noção de corpo abstracto

Diz-se que, num dado conjunto M de elementos quaisquer, é definida uma operação θ, binária e unívoca, quando exista uma lei que faça corresponder a cada par ordenado a, b de elementos de M, um, e um só, elemento $c = a \theta b$, também de M.

Se M fôr o conjunto dos números racionais, sabemos que são definidas em M duas operações — a adição $(+)$ e a multiplicação $(\ )$ — gozando das seguintes propriedades fundamentais (por a, b, c designamos elementos arbitrários de M):

Para a adição:

R_1) $(a+b)+c=a+(b+c)$ (associatividade)

R_2) $a+b=b+a$ (comutatividade)

R_3) Existe em M um elemento 0 tal que $a+0=a$

R_4) Para cada elemento a, existe um elemento $-a$, também de M, tal que $a+(-a)=0$.

Para a multiplicação:

R_5) $(a \cdot b)\ c=a\ (b \cdot c)$ (associatividade)

R_6) $a\ b=b \cdot a$ (comutatividade)

R_7) Existe em M um elemento 1 tal que $a \cdot 1=a$

R_8) Para cada elemento $a \neq 0$, existe um elemento a^{-1}, também de M, tal que $a \cdot a^{-1}=1$.

Mixtas:

R_9) $(a+b) \cdot c=a \cdot c+b \cdot c$ (distributividade)

R_{10}) Se N é um conjunto de elementos de M tal que: 1) N contém 1; 2) dados dois elementos a, b de N (sendo $b \neq 0$), também $a+(-b)$ e $a \cdot b^{-1}$ pertencem a N, então N coïncide com M.[1]

Além destas operações, é definida em M uma relação binária (relação de ordem «>») que satisfaz às seguintes condições:

R_{11}) Dados dois elementos a, b de M, uma, e uma só, das hipóteses $a>b$, $a=b$, $b>a$ se verifica necessàriamente.

R_{12}) Se $a \geq b$ e $c \geq 1$ ou $c>0$, tem-se $a+c>b$ e $ac \geq bc$.[2]

[1] A restrição «N contém 1» pode ser substituída por esta outra «N contém pelo menos dois elementos».

[2] Supõe-se, é claro, que já foi definida a relação «$a \geq b$» como equivalente a «$a>b$ ou $a=b$». A hipótese $c \geq 1$ poderia ser suprimida, acrescentando a condição $1>0$, para completar a caracterização.

É fácil demonstrar que as propriedades R_1 a R_{12} *caracterizam* os números racionais, isto é, que *tôdas* as proposições relativas a números racionais se podem deduzir lògicamente das condições R_1 a R_{12}. Em tudo o que segue, representaremos por R_a o conjunto dos números racionais.

Interessa observar que, suprimindo no sistema R_1 a R_{12} a condição R_8, e modificando a condição R_{10} com a supressão de $a \cdot b^{-1}$, se obtém um sistema de condições, *caracteristico* do conjunto I_n dos números inteiros relativos (isto é, positivos e negativos); e que, suprimindo ainda as condições R_3 e R_4, e modificando R_{10} com a substituïção de $a+(-b)$ por $a+b$, ou mesmo por $a+1$ (feita já a supressão de $a \cdot b^{-1}$), se obtém *uma caracterização* do conjunto N_n dos números naturais. Dêste modo se vê, em particular, que a condição R_{10} não é mais do que uma modificação do princípio da indução completa, relativo aos números naturais.

Substituamos agora R_{10} pela condição mais fraca: R^*_{10}) Se N fôr um subconjunto de M tal que: 1) N contém pelo menos um elemento (ou seja, *não é vazio*); 2) qualquer que seja o elemento a de N, também $a+1$ pertence a N, — então, dado um elemento b de M, ou b pertence a N, ou existe em N um elemento maior do que b (princípio de Arquimedes modificado).

O novo sistema $R_1 - R_9$, R^*_{10}, R_{11}, R_{12} já não é verificado sòmente em R_a: é-o também no conjunto R_e dos números reais; no conjunto dos números da forma $a+b\sqrt{2}$, com a, b racionais; no conjunto dos números da forma $f(\log 2)$, sendo f uma função racional de coeficientes racionais e $\log 2$, por exemplo, o logaritmo ordinário (real) de 2, etc. É fácil reconhecer que, entre todos os conjuntos de números que satisfazem a tal sistema de propriedades, o conjunto R_e é, *de certo modo*, o máximo.[3] Podemos, no entanto, obter uma caracterização *directa* do conjunto R_e, juntando ao último grupo de condições, esta outra:

R_{13}) Dados dois sub-conjuntos não vazios A e B de M, tais que todo o elemento de A é maior do que qualquer elemento de B, existe em M, *pelo menos*, um elemento k (elemento separador) tal que: 1) k é igual ou maior do que qualquer elemento de B; 2) qualquer elemento de A é igual ou maior do que k (forma fraca do princípio de Dedekind-Cantor).

Suprimamos nêste último sistema a condição R^*_{10}. O conjunto R_e será, *de certo modo*, o mínimo conjunto aditivo, multiplicativo e ordenado, que satisfaz ao novo sistema. Em vez de averiguar da existência de outros conjuntos que verifiquem porventura as mesmas condições, suprimamos a condição R_{13}, isto é, passemos a considerar o sistema $R_1 - R_9$, R_{11}, R_{12}. Tal sistema será verificado, por exemplo, no conjunto das funções racionais em uma variável x (variável real ou variável racional ou possìvelmente de outra natureza) de coeficientes reais (ou racionais, etc.), com a noção ordinária de produto e a soma de funções racionais e com o seguinte critério de ordenação: *a)* dados dois polinómios $p(x)$ e $q(x)$, supostos ordenados segundo as potências crescentes de x, ter-se-à $p > q$, quando e só quando se tiver $a_i > b_i$ sendo a_i o primeiro coeficiente de $p(x)$ que não é igual ao coeficiente correspondente b_i de $q(x)$; *b)* dadas duas funções racionais $\frac{p}{q}, \frac{r}{s}$ (com $q>0$, $s>0$) ter-se-à $\frac{p}{q} > \frac{r}{s}$ quando e só quando $ps > qr$. Êste conjunto fica por tal processo ordenado, mas não arquimedianamente ordenado, visto que não se verifica nêle a condição R^*_{10}; assim, por exemplo, entre o número 3 e todos os números racionais maiores do que 3 (considerados os números como polinómios do grau zero) estará compreendido o elemento $3+2x$; o elemento $3+\frac{x}{2}-x^2$. etc.; para lá de todos os números racionais, existirão outros elementos como $\frac{1}{x}$, etc. É-se dêste modo conduzido a uma teoria análoga à dos infinitésimos de ordem inteira (positiva ou negativa). As considerações anteriores são ainda aplicáveis, *mutatis mutandis*: *a)* aos conjuntos das funções racionais, em mais de uma variável; *b)* aos conjuntos das funções meromorfas, reais, em uma ou mais de uma variáveis, com um mesmo domínio de existência.

Examinemos agora o conjunto K dos números complexos ou mesmo o conjunto dos números da forma $a+bi$ com a e b racionais (corpo de números de Gauss). Em tais conjuntos são definidas igualmente uma adição e uma multiplicação que verificam as condições $R_1 - R_9$ (mas não a condição R_{10}). Seria possível definir em tais conjuntos uma relação de ordem que satisfizesse a R_{11}, mas tal relação já não satisfaria certamente a R_{12}: o seu interêsse seria portanto muito reduzido.

Em quási todos os exemplos anteriores (exceptuando os casos de I_n e de N_n), o núcleo de condições $R_1 - R_9$ é respeitado. Estas condições, de carácter puramente operatório (regras de cálculo), são as mais interessantes, do ponto de vista algébrico. Pois bem:

[3] O sentido da expressão «de certo modo» será precisado com a noção de *isomorfismo*, em um outro artigo que espero poder publicar nesta revista. Encontrar-se-á adiante a definição do isomorfismo num caso particular.

DEFINIÇÃO — *Chama-se «corpo» ou «domínio de racionalidade» a todo o conjunto* M *de elementos quaisquer, em que sejam definidas duas operações binárias e unívocas — a uma das quais convencionaremos dar o nome de adição* $(+)$, *e à outra o nome de multiplicação* $(\cdot)$ *— gozando das propriedades* $R_1 - R_9$. [4]

Fàcilmente se demonstra que: Para que um sub-conjunto N dum corpo M seja também um corpo relativamente às duas operações definidas em M, é necessário e suficiente que: 1) N contenha 1; 2) dados dois elementos a, b de N (sendo $b \neq 0$), também $a+(-b)$ e ab^{-1} pertençam a N. Se tal condição se verifica, diremos que N é um sub-corpo de M. Podemos agora dar à condição R_{10} *verificada no corpo racional*, a forma seguinte:

R_{10}) Se N é um sub-corpo de M, tem-se $N=M$.

Portanto, R_a admite um único sub-corpo: R_a.

Até aqui, temos visto apenas exemplos de corpos *infinitos*, isto é, de corpos com uma infinidade de elementos. Mas existem porventura corpos *finitos*? A esta pregunta vamos procurar responder.

Como se sabe, diz-se que dois números inteiros relativos a, b são congruentes em relação a um módulo p (sendo p também um inteiro relativo) e escreve-se $a \equiv b\ (p)$ quando $a-b$ é um múltiplo de p. Seja $p=3$, e representemos, em geral, por $[a]$ a classe de todos os números congruentes ao número a, em relação ao módulo 3; se fôr a' o resto da divisão de a por 3 ter-se-à, evidentemente $[a]=[a']$, visto que $a \equiv a'\ (3)$, e chamaremos a $[a']$ forma canónica de classe $[a]$. Por exemplo: $[7]=[4]=[-2]=[1]$: a forma canónica desta classe será $[1]$. O conjunto I_n dos inteiros relativos ficará assim *repartido* [5] em 3 classes (*classes-resto para o módulo* 3): $[0]$, $[1]$, $[2]$; e entre tais classes podem-se definir naturalmente uma adição e uma multiplicação do modo seguinte: $[a]+[b]=[a+b]$, $[a]\cdot[b]=[a\cdot b]$ [6] Aplicando êste critério, e fazendo a redução à forma canónica, podemos construir as duas tabelas seguintes:

Tábua da adição

	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

Tábua da multiplicação

	[0]	[1]	[2]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]
[2]	[0]	[2]	[1]

Fàcilmente se vê que tôdas as condições $R_1 - R_9$ são verificadas por tais operações. Em particular, $[0]$ é aqui o módulo da adição e $[1]$ o módulo da multiplicação. Trata-se portanto dum corpo e, precisamente, dum corpo finito. Exemplos análogos se podem obter considerando as classes-resto em relação a qualquer módulo primo p.

É curioso observar que todos êstes corpos finitos verificam a condição R_{10}. Demonstra-se que, dado um corpo Ω, existe sempre um sub-corpo mínimo de Ω, isto é, um corpo Γ contido em todos os sub-corpos de Ω; e que êste corpo mínimo Γ ou é isomorfo [7] ao corpo R_a ou é isomorfo ao corpo das classes-resto em relação a um módulo primo p. No primeiro caso diz-se que Ω tem a característica zero, no segundo caso diz-se que tem a característica p.

Mas ocorre ainda preguntar: O que sucede quando o módulo das congruências não fôr primo? As classes-resto não constituem neste caso um corpo? É o que veremos adiante.

Anéis; domínios de integridade

Consideremos o conjunto das classes-resto em relação ao módulo 6. Definindo nêste conjunto uma adição e uma multiplicação em modo análogo ao que fizemos anteriormente quando se tratava do módulo 3, ver-se-à que as condições $R_1 - R_9$ são tôdas verificadas, excepto a condição R_8; porque, por exemplo, não existe o inverso de $[2]$, isto é, não existe naquêle conjunto nenhum elemento $[x]$ tal que $[x]\cdot[2]=[1]$ (não é sempre possível a divisão por um número diferente de 0).

Consideremos de novo o conjunto I_n: já vimos que são nêle definidas uma adição e uma multiplicação

[4] Suprimindo a condição R_8 chega-se à noção de «corpo assimétrico» (*Schiefkörper*, na terminologia de Van der Waerden). Abandonámos, nêste ponto, a noção de *ordem*. Ela dá origem à noção de limite, e é portanto o ponto de partida para a Análise, para a Topologia.

[5] Diz-se que um conjunto M está *repartido* em sub-conjuntos $A_1, A_2, \cdots$ quando, dado um elemento a de M, a pertence necessàriamente a um dêstes sub-conjuntos e não pode pertencer a dois dêles ao mesmo tempo.

[6] Já conhecíamos um exemplo dum corpo cujos elementos são representáveis por classes de elementos dum outro conjunto. Com efeito, todo o número racional pode ser definido por uma infinidade de pares de números inteiros, sendo $[a,b]=[c,d]$ se, e só se, $ad=bc$. Reduzir uma fracção à «forma canónica» é reduzi-la à sua «expressão mais simples».

[7] Diz-se que dois corpos Δ e Ω são isomorfos quando se pode estabelecer entre êles uma correspondência biunívoca que respeite a adição e a multiplicação, isto é, uma correspondência biunívoca tal que, se forem a, b dois elementos arbitrários de Δ e a', b' os elementos correspondentes de Ω, à soma $a+b$, corresponde em Ω a soma $a'+b'$, ao produto $a\cdot b$ corresponde em Ω o produto $a'\cdot b'$.

que verificam as condições $R_1 - R_7$, R_9, mas não a condição R_8. Se, em vez do conjunto dos inteiros relativos, considerarmos o conjunto dos números pares (positivos e negativos) — com a adição e a multiplicação definidas em I_n — vê-se que não só a condição R_8, mas também a condição R_7, se deixa de verificar.

DEFINIÇÕES — *Chama-se «anel» a todo o conjunto em que são definidas uma adição e uma multiplicação satisfazendo às condições* $R_2 - R_5$, R_9; *«anel comutativo» a todo o anel em que é verificada a condição* R_6; *«anel comutativo com unidade», a todo o anel comutativo em que é verificada a condição* R_7.

Um outro exemplo de anel comutativo, além dos que já foram apresentados, é-nos fornecido pelo conjunto C_n das funções contínuas num mesmo intervalo (a, b), sendo a multiplicação e a adição ali definidas do seguinte modo:

$f+g=h$ equivalente a $f(x)+g(x) \equiv h(x)$;
$f \cdot g=h$ equivalente a $f(x) \cdot g(x) \equiv h(x)$.

Êste anel possui uma unidade, que é representada pela função $\varphi(x) \equiv 1$.

O interêsse da teoria dos anéis reside principalmente no facto de nêles não ser necessàriamente verificada a condição R_8 (de não ser sempre possível a divisão por um número diferente de zero) — o que dá origem ao conceito de divisibilidade e bem assim a noções correspondentes às de máximo divisor comum, menor múltiplo comum, números primos, etc.[8] Importa notar que o problema correspondente ao da decomposição dum número em factores primos, e o de averiguar em que condições tal decomposição é única (àparte a ordem) — constituem o principal assunto da teoria dos anéis; do mesmo modo que o problema central da teoria dos corpos consiste em averiguar a que condições deve satisfazer um corpo para que nêle seja válida a teoria de Galois (relativa à resolubilidade das equações algébricas por meio de radicais).

No conjunto I_n (e anàlogamente no conjunto dos números pares, dos múltiplos de 3, etc.), não é verificada a condição R_8 — mas é verificada a condição mais fraca:

R_8^*) Se $ab=ac$ e $a \neq 0$, tem-se $b=c$. *Ou ainda, o que é equivalente:* se a equação $ax=b$ admite uma solução, essa solução será única.

Nos outros dois exemplos, que apresentámos, de anéis comutativos — anel das classes-resto par ao módulo 6 e conjunto C_n — a condição R_8^* não é respeitada. Por exemplo, no primeiro dêstes anéis tem-se $[2] \cdot [5] = [2] \cdot [2]$ e $[2] \neq [0]$, sem que se tenha $[5] = [2]$.

DEFINIÇÃO — *Chama-se domínio de integridade a todo o anel comutativo que satisfaz à condição* R_8^*.

Um exemplo de domínio de integridade, além dos que já foram apresentados, é-nos oferecido pelos conjuntos de polinómios em uma ou mais variáveis e de coeficientes situados num dado corpo. Uma propriedade interessante dos domínios de integridade, que deriva imediatamente da condição R_8^* (é-lhe mesmo equivalente) é a seguinte: uma equação algébrica de grau n, de coeficientes situados num domínio de integridade I, não pode ter em I mais de n raízes. Daqui resulta que dois polinómios em x, de coeficientes situados em I, de grau não superior a n que tomem o mesmo valor para mais de n valores distintos de x, tem os coeficientes respectivamente iguais (princípio das identidades). Esta propriedade não se verifica nos anéis que não satisfazem à condição R_8^*.

Noção de grupo

Diz-se que um conjunto abstracto M, *em que é definida uma operação* θ, *binária e unívoca, constitui um grupo em relação a* θ, quando são verificadas *as seguintes condições* (a, b, c representam elementos arbitrários de M):

G_1) $(a\theta b)\,\theta c = a\theta(b\theta c)$ (associatividade)
G_2) Existe em M um elemento u tal que $a\theta u = a$
G_3) Dado um elemento a, existe em M um elemento $\varphi(a)$ tal que $a\theta\varphi(a) = u$.

Se além destas é verificada a condição:

G_4) $a\theta b = b\theta a$ (comutatividade),

diz-se que M é um grupo comutativo ou abeliano.

Vê-se imediatamente que todo o corpo constitui um grupo comutativo relativamente à adição e, o mesmo, se excluirmos o zero, relativamente à multiplicação. Quando num grupo não fôr definida mais de uma operação binária, podemos adoptar para esta o nome de multiplicação, escrevendo $a \cdot b$ em vez de $a\theta b$, 1 em vez de u, a^{-1} em vez de $\varphi(a)$ (notação multiplicativa); ou o nome de adição, escrevendo $a+b$ em vez de $a\theta b$, 0 em vez de u, $-a$ em vez de $\varphi(a)$ (notação aditiva). Trata-se apenas, claro está, duma questão de comodidade.

Fàcilmente se demonstra que, para que um sub-conjunto H dum grupo G constitua também um grupo relativamente à mesma operação definida em G, é necessário e suficiente que (adoptando a notação aditiva), dados dois elementos arbitrários a, b de H, a diferença $a+(-b)$ pertença também a H. Se tal condição se verifica, diz-se que H é um sub-grupo de G. Então, o princípio correspondente ao da indução completa para o anel dos inteiros I_n pode enun-

[8] **Para um estudo destas questões em tôda a sua generalidade, convém introduzir uma outra noção — a noção de «ideal» — que me abstenho de apresentar aqui, para não tornar mais longo êste artigo.**

ciar-se dêste modo: «Se N fôr um sub-grupo aditivo de M, tem-se $N=M$».

Um exemplo típico de grupo é-nos dado pelos conjuntos de transformações. Chama-se transformação biunívoca dum conjunto A em si mesmo a tôda a operação t que faça corresponder a cada elemento x de A um, e um só elemento $y=t(x)$ também de A, de modo que: *a)* elementos distintos de A sejam transformados por t em elementos distintos de A; *b)* dado um elemento y_1 de A, existe sempre um elemento x_1 de A tal que $y_1=t(x_1)$. *Convencionemos* chamar *produto* de duas transformações biunívocas s, t do conjunto A em si mesmo (pela ordem em que estão representadas) à transformação st que resulta de executar primeiro t e depois s. isto é, transformação st tal que $st(x)=s[t(x)]$, qualquer que seja o elemento x de A. É fácil ver que esta *multiplicação* satisfaz às condições G_1-G_3, e que, portanto, o conjunto Σ das transformações biunívocas dum conjunto A em si mesmo constitui um grupo relativamente a tal operação. Em particular, a unidade é aqui representada pela *identidade*, isto é, por aquela transformação que deixa fixos todos os elementos de A; e a transformação inversa t^{-1} duma dada transformação t será definida pela condição: $t^{-1}[t(x)]=x$, qualquer que seja x.

Por exemplo, as transformações biunívocas do conjunto R_e em si mesmo são representadas por aquelas funções reais de variável real que admitem uma função inversa. Consideremos, no conjunto τ de tais funções, o conjunto Γ das funções contínuas: tal conjunto Γ coïncide, visìvelmente, com o conjunto das funções crescentes e das funções decrescentes; e é fácil reconhecer que o conjunto Γ constitui um sub-grupo de τ, relativamente à multiplicação que definimos para as transformações.[9] Porém, o grupo Γ não é comutativo, como resulta do seguinte exemplo: Sejam as funções $\varphi(x)\equiv x^3$, $\psi(x)\equiv 1-x$ (crescente e primeira, decrescente e segunda); tem-se, por um lado, $\varphi[\psi(x)]\equiv[\psi(x)]^3\equiv(1-x)^3$, e, por outro lado, $\psi[\varphi(x)]\equiv 1-\varphi(x)\equiv 1-x^3$. Êste exemplo mostra que os grupos de transformações não são geralmente comutativos.

Notemos ainda que o conjunto das funções crescentes constitui um sub-grupo de Γ, relativamente à operação considerada.

A Geometria fornece-nos exemplos notáveis de grupos de transformações. O conjunto das translações, o conjunto das rotações em relação a um eixo (ou em relação a um ponto), o conjunto das simetrias em relação a um plano, o conjunto das homotetias em relação a um ponto — constituem grupos de transformações, e todos êstes grupos estão contidos no grupo das semelhanças, característico da geometria euclidiana. Anàlogamente, as afinidades, as projectividades, as correlações. etc., formam grupos de transformações. Deve-se a Felix Klein a ideia (apresentada no célebre programa de Erlangen) de caracterizar as geometrias por meio de grupos de transformações.[10]

Notemos, por último, que, se o conjunto A é finito, às transformações biunívocas de A em si mesmo se dá o nome de substituïções. Os grupos de substituïções desempenham um papel fundamental na teoria de Galois; historicamente, representam o primeiro passo para a formulação explícita do conceito de grupo.

PROBLEMAS PROPOSTOS

1 — Caracterização do corpo dos números da forma $a+b\sqrt{2}$, com a, b racionais, por meio da adição, da multiplicação e da relação $>$. Construção abstracta dêste corpo a partir do corpo racional.

2 — Idem para o corpo dos números da forma $f(\log 2)$, sendo $\log 2$ o logaritmo ordinário (real) de 2 e f uma função racional de coeficientes situados no corpo a que se refere o problema 1.

3 — Idem, para o corpo de números de Gauss (introduzindo de um modo adequado a relação $>$).

4 — Idem, para o corpo complexo.

5 — Averiguar se existem corpos ordenados *diferentes* de R_e[11] que verifiquem as condições R_{11}, R_{12}, R_{13} (no caso negativo, a condição R_{10}^* — princípio de Arquimedes — será supérflua na caracterização, que nêste artigo foi apresentada, do corpo real).

6 — Demonstrar que o anel C_n das funções contínuas, definidas num mesmo intervalo (a, b), não constitui um domínio de integridade.

Nota — A resolução dêstes problemas parece-nos bastante recomendável para a iniciação do leitor nos métodos da Matemática moderna. Publicarei soluções dos mais interessantes num futuro número desta revista.

Roma, Março de 1944.

---

[9] Esta definição do produto não é a mesma que considerámos atrás, ao definir a forma C_n das funções contínuas num intervalo.

[10] Um outro exemplo importante é o do grupo dos automorfismos dum corpo. Chama-se automorfismo dum corpo Ω a todo o isomorfismo de Ω em si mesmo. Demonstra-se fàcilmente que os automorfismos dum corpo formam um grupo de transformações. O corpo R_a admite um só automorfismo: a identidade. O corpo dos números de Gauss (números de forma $a+bi$, com a e b racionais) admite, alèm da identidade, o automorfismo que transforma $a+bi$ no seu conjugado $a-bi$.

[11] Em vez de «diferentes de R_e», seria mais correcto escrever «não isomorfos a R_e». No entanto, o corpo R_e pode considerar-se definido *a menos de um isomorfismo*.