

Resumo de discussões conduzidas nas aulas de MAT036.

Idéias preliminares —

- Seja C um conjunto de objetos (reais ou ideais). Uma relação $\mathbb{R}$ entre os elementos de C pode gozar das propriedades seguintes:
 - a) REFLEXIVIDADE, se todo elementos x de C satisfizer a $x \mathbb{R} x$.
 - b) SIMETRIA, se, sempre que dois quaisquer elementos a e c satisfizerem à condição $a \mathbb{R} c$, também satisfizerem à condição $c \mathbb{R} a$.
 - c) TRANSITIVIDADE, se sempre que três quaisquer elementos a , x e c satisfizerem (simultaneamente) às condições $a \mathbb{R} x$ e $x \mathbb{R} c$, também a e c satisfizerem à condição $a \mathbb{R} c$.
- Problema: Verifique quais as propriedades das relações seguintes:
 - a) A relação SER FILHO DE.
 - b) A relação SER PAI DE.
 - c) A relação SER IRMÃO DE.
 - d) A relação SER CUNHADO DE.
 - e) A relação SER MAIS ALTO QUE.
 - f) A relação SER CONTERRÂNEO DE.
 - g) A relação SER DELEGADO DE.
- Diremos que uma relação é uma equivalência, se ela gozar das três propriedades REFLEXIVIDADE, SIMETRIA e TRANSITIVIDADE. Habitualmente, designamos uma equivalência por $\equiv$.

Classificação —

- Diremos que um conjunto C está (exaustivamente) classificado, se for especificado um critério que permita separá-los em partes, que gozem das propriedades seguintes:
 - a) C é a reunião de todas as partes. Em notação usual, $C = \bigcup P_i$, $i \in J$. (J é denominado conjunto de índices.) Isso significa que todo elemento x de C está classificado, isto é, dado x em C , existe um índice i em J tal, que $x \in P_i$.
 - b) Duas partes quaisquer são disjuntas. Se o não forem, coincidirão. Em notação usual, dados dois índices quaisquer h e k , ou $P_h = P_k$ ou $P_h \cap P_k = \emptyset$ (sua interseção é vazia).

c) Nenhuma parte é vazia.

- As partes especificadas pelo critério de classificação são denominadas CLASSES.

Lema — A instituição de uma **equivalência** $\equiv$ em um conjunto C permite classificar os elementos de C .

De fato, designemos por $[p]$ a parte de C constituída dos elementos que são equivalentes ao elemento p . Em notação usual, $[p] = \{x \in C : x \equiv p\}$.

É fácil verificar que as partes assim definidas operam a classificação de C .

- Com efeito, dado qualquer elemento a de C , podemos afirmar que $a \in [a]$. (Porquê?) Isso significa que todos os elementos de C estão classificados.
- Dados dois elementos a e b de C , ou $[a] = [b]$ ou $[a] \cap [b] = \emptyset$. (Porquê?)
- Finalmente, decorre da definição de $[p]$, que $[p]$ não é vazio.

Quando classificamos os elementos de um conjunto mediante uma equivalência, as partes obtidas são denominadas **CLASSES DE EQUIVALÊNCIA** e o conjunto de tais classes é designado **CONJUNTO QUOCIENTE** (do conjunto C pela equivalência).

Uma classificação dos números inteiros —

Escolhamos e fixemos um número inteiro estritamente positivo, ao qual chamaremos módulo e o qual denotaremos por m .

Dados dois números inteiros a e c , diremos que a e c **são congruentes segundo o módulo m** , se, divididos por m , apresentarem o mesmo resto. Adotaremos a notação seguinte, para indicar que os números inteiros a e c são congruentes segundo o módulo m : $a \equiv c \pmod{m}$.

Um modo equivalente de se definir a congruência entre dois números inteiros decorre das considerações seguintes. No que tange à divisão por m , os números a e c podem ser representados como $a = mq_1 + r_1$ e $c = mq_2 + r_2$. Logo, se $a \equiv c \pmod{m}$, então $c - a = m \cdot (q_2 - q_1)$. Isso significa que $a \equiv c \pmod{m}$ se, e somente se, $c - a$ for um múltiplo de m . Por isso, poderemos, doravante, dizer que $a \equiv c$ e, e somente se, $c - a$ for um múltiplo de m .

Essa definição torna ainda mais fácil verificar que a congruência de dois números inteiros segundo um dado módulo m constitui uma equivalência no anel dos números inteiros. De fato:

- Reflexividade: Para todo número inteiro x , $x - x = 0$. Logo, $x \equiv x \pmod{m}$.
- Reciprocidade: Dados dois quaisquer números inteiros a e c , se $a \equiv c \pmod{m}$, então $c - a$ será múltiplo de m ; logo, também $a - c$ será múltiplo de m . Portanto, $c \equiv a \pmod{m}$.
- Transitividade: Dados três quaisquer números inteiros a , c e x , se $a \equiv x \pmod{m}$, então $x - a = rm$ (para algum número inteiro r); se $x \equiv c \pmod{m}$, então $c - x = sm$ (para algum número inteiro s). Somando membro a membro, obtemos $c - a = (r + s)m$, o que equivale a $a \equiv c \pmod{m}$.

De acordo como o que foi exposto, a congruência (segundo um certo módulo) entre dois números inteiros constitui uma equivalência definida no anel dos números inteiros. Ainda segundo o que foi exposto, tal equivalência institui uma classificação no anel dos números inteiros. Nesse caso, haverá exatamente m classes de equivalência (ou, equivalentemente, será igual a m a cardinalidade do conjunto quociente do anel dos números inteiros pela relação considerada). Esse conjunto quociente será denotado por $\mathbb{Z}/(m)$.

Dado um conjunto não vazio C , chamamos **lei de composição interna** (ou, com menor precisão, uma **operação**) a uma correspondência unívoca entre $C \times C$ e C (isto é, a uma função que a cada par de elementos de C associa um elemento de C).

Definiremos uma multiplicação em $\mathbb{Z}/(m)$, associando ao par (a, c) de números inteiros o resto, denotado por $a.c$ (ou, mais comodamente, por ac), da divisão de $a.c$ por m .

Note-se que foi adotada uma linguagem pouco exata, na definição anterior. De fato, a lei de composição interna que pretendemos definir não associa números inteiros a pares de números inteiros. Na verdade, ela associa classes de equivalência a pares de classes de equivalência. De fato, o conjunto quociente do anel dos números inteiros pela relação de congruência não é um conjunto de números inteiros mas um conjunto de classes de equivalência.

Mas, para facilitar o tratamento desse tema, podemos escolher como representante de cada classe de equivalência um qualquer número inteiro a ela pertencente. Para isso, é suficiente

mostrarmos que, escolhidos dois quaisquer números inteiros a e b em uma classe M_1 e dois quaisquer números inteiros c e d em uma classe M_2 , são iguais os restos obtidos na divisão de ac e de bd por m . Por isso, doravante, em vez de nos referirmos ao produto de duas classes de equivalência, falaremos simplesmente no produto de dois números inteiros segundo o módulo m .

Verificamos que uma tal multiplicação goza das propriedades seguintes:

- Associatividade — É intuitivo que, como a multiplicação de números inteiros é associativa, também o será a multiplicação de tais classes de equivalência, pois o produto de duas quaisquer classes de equivalência pode ser examinado, considerando-se apenas o produto de seus respectivos representantes, que são números inteiros.
- Existência de elemento neutro — A classe de equivalência que contém o número inteiro 1 (e que, portanto, pode ser por ele representada) desempenha o papel de unidade.
- Existência de elementos inversos — Dizemos que dois números inteiros são relativamente primos, se for igual a 1 o seu maior divisor comum. Podemos mostrar que é inversível toda classe representável por um número inteiro z tal, que z e m sejam relativamente primos.

Assim, o conjunto das classes inversíveis apresenta estrutura de grupo. (Na verdade, tal grupo é comutativo, fato esse de comprovação análoga à prova da associatividade da multiplicação.) Tal grupo será denotado por $(\mathbb{Z}/(m))^*$.

Uma discussão sobre a geometria do plano (parabólico) —

No presente escrito, retornaremos à fase histórica anterior à publicação por Moritz Pasch de suas *Vorlesungen über neuere Geometrie* (1882) e recorreremos tanto à intuição quanto ao modelo que será adotado para a teoria formal vertente. Nosso escopo é perceber, por vivência, do que se trata, quando dizemos, por exemplo, que “Bolzano não propõe essa nova prova por desconfiar das anteriores, fundada em argumentos geométricos”.

Diremos que um ponto qualquer sobre uma reta a decompõe em duas [semi-retas](#). Ao nos referirmos a uma dessas semi-retas, diremos que ela nasce no ponto considerado.

Uma reta decompõe o plano em dois **semiplanos**. Também duas semi-retas que nascem no mesmo ponto decompõem o plano em duas partes, que serão denominadas **ângulos**. A esse ponto chamaremos **vértice do ângulo** e às duas semi-retas chamaremos **lados do ângulo**.

Suporemos primitiva a noção de **ângulos congruentes**. Suporemos, além disso, que a congruência entre ângulos seja uma relação de equivalência. (Castrucci, p. 126)

Diremos que dois pontos distintos determinam **um segmento** sobre a reta que passa por eles e diremos que tais pontos são as extremidades do segmento vertente. Além disso, suporemos primitiva a noção de **segmentos congruentes**. Suporemos, além disso, que a congruência entre segmentos seja uma relação de equivalência.

Se um mesmo ponto for extremidade comum a dois segmentos distintos de reta, também diremos que esses segmentos determinam o ângulo vertente.

Chamaremos **triângulo** à parte do plano determinada por três pontos distintos e pelas três retas definidas por esses pontos (considerados dois a dois). A esses três pontos chamaremos **vértices do triângulo** e chamaremos **lados do triângulo** aos segmentos das retas consideradas, determinados pelos vértices (considerados dois a dois). Aos ângulos que contém um triângulo, cujos vértices sejam vértices do triângulo e cujos lados contenham lados do triângulo chamaremos **ângulos (internos)** do triângulo. Consideraremos intuitiva a noção de **ângulo oposto a um lado**.

Dados dois triângulos, de vértices A, B e C e L, M e N, respectivamente, diremos que esses dois triângulos são congruentes, se existir uma correspondência biunívoca (ou bijetiva) σ entre o conjunto de vértices do primeiro triângulo e conjunto de vértices do segundo triângulo, de modo que, quando dois vértices forem congruentes, também o serão os lados opostos (Moise, p. 83). Com maior exatidão, diremos que um triângulo é congruente com o triângulo de vértices A, B e C, se existir uma bijeção σ entre o conjunto de vértices $\{A, B, C\}$ e o conjunto dos vértices do primeiro triângulo, de sorte que sejam congruentes o segmento cujas extremidades são A e B e o segmento cujas extremidades são $\sigma(A)$ e $\sigma(B)$; que sejam congruentes o segmento cujas extremidades são B e C e o segmento cujas extremidades são $\sigma(B)$ e $\sigma(C)$; que sejam congruentes o segmento cujas extremidades são C e A e o segmento cujas extremidades são $\sigma(C)$ e $\sigma(A)$; e que sejam congruentes os ângulos (internos) cujos vértices são A e $\sigma(A)$, os

ângulos (internos) cujos vértices são B e $\sigma(B)$ e os ângulos (internos) cujos vértices são C e $\sigma(C)$.

Axioma — Um triângulo T_1 é congruente com um triângulo T_2 , se dois lados do primeiro forem respectivamente congruentes com dois lados do segundo e se, além disso, forem congruentes os ângulos (internos) determinados por esse lados. (Esse axioma é informalmente denominado caso LAL.)

Teorema — Se forem congruentes dois lados de um mesmo triângulo, então serão congruentes os ângulos (internos) que se opõem a esses lados.

Corolário — Todo triângulo equilátero é equiângulo.

Teorema — Um triângulo T_1 é congruente com um triângulo T_2 , se dois ângulos (internos) do primeiro forem respectivamente congruentes com dois ângulos (internos) do segundo e se, além disso, forem congruentes os lados cujas extremidades, em cada triângulo, são os vértices dos ângulos (internos) considerados. (Esse axioma é informalmente denominado caso ALA.)
