Sociedade Brasileira de Matemática - SBM

Universidade Federal do Acre - UFAC

Mestrado Profissional em Matemática - PROFMAT

Henrique Hiroto Yokoyama

A Estrutura Algébrica dos Vértices de um Polígono Regular

Julho – 2015

Sociedade Brasileira de Matemática - SBM

Universidade Federal do Acre - UFAC

Mestrado Profissional em Matemática - PROFMAT

A Estrutura Algébrica dos Vértices de um Polígono Regular

Trabalho de Conclusão de Curso apresentado ao Mestrado Profissional em Matemática em Rede Nacional – PROFMAT, no de Rio Branco – AC, como requisito **para a obtenção do título de mestre em Matemática**.

Orientador: prof. Dr. José Ivan da Silva Ramos

Julho – 2015

A Estrutura Algébrica dos Vértices de um Polígono Regular

Dissertação apresentada ao Programa de Pós-Graduação de Mestrado Profissional em Matemática em Rede Nacional (PROFMAT), do Centro de Ciências Exatas e Tecnológicas da Universidade Federal do Acre (Ufac), como requisito parcial para a obtenção do título de Mestre em Matemática.

BANCA EXAMINADORA

Prof. Dr. José Ivan da Silva Ramos
(Presidente - Orientador)

Prof. Dr. Tomás Daniel Menéndez Rodríguez
(Avaliador Externo - UNIR)

Prof. Me. Cleber Pereira
(Membro - UFAC)

Local: Laboratório de Didática do curso de Matemática, no campus sede da Ufac.

Rio Branco, 24 de julho de 2015.

Dedico esta dissertação

À minha esposa Marília Yokoyama; à minha família, em especial a minha mãe Tamiko Yokoyama e a meu pai Hirofumi Yokoyama (*IN MEMORIAN*).

Agradecimentos

Ao meu pai, Hirofumi Yokoyama (*IN MEMORIAM*) pela vida dedicada a seus filhos, transferindo grandes valores de dignidade e honra para minha vida.

À minha mãe, Tamiko Yokoyama, a quem devo TUDO que há de melhor na minha essência de vida.

À minha linda esposa, Marília Hadad Rocha Yokoyama, que amo incondicionalmente, sempre me motivando com seu sorriso, abraços e demonstrações de amor e carinho. Creditando sua confiança, tendo paciência comigo nesse período de estudos para o mestrado e que faz com que nossos olhares sempre se voltem a uma mesma direção.

À minha irmã Chiemi Yokoyama e ao meu irmão Takashi Yokoyama, que muitas vezes serviu-me de referência para que eu pudesse sempre ir mais alto.

Ao Professor Dr. José Ivan da Silva Ramos, meu orientador, pela disponibilidade, competência, dedicação, amizade e paciência, idealizador do trabalho e grande parâmetro de excelência profissional.

Aos colegas de mestrado pela troca de experiências e conhecimentos que fizeram jus ao termo coletividade, em especial, para Mara Rykelma da Costa Silva, Ricardo Moura da Silva e Leylane Ferreira Hadad, grande amiga e parceira de longas datas.

Ao amigo Uelder Araújo Teixeira, pelas palavras de motivação e companheirismo.

Ao Mestrado Profissional em Matemática em Rede Nacional (PROFMAT), à Universidade Federal do Acre (UFAC) e todos os professores do curso, por contribuírem com a minha formação. Especialmente os professores Dr. Edcarlos Miranda De Souza, Me. Sandro Ricardo Pinto da Silva e Ma. Daiana dos Santos Viana que atuaram com muita dedicação nas aulas ministradas.

À Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) que permitiu a realização deste trabalho, concedendo-me bolsa de estudos.

E a todos que direta ou indiretamente contribuíram para que fosse possível a realização deste Trabalho de Conclusão de Curso.

Resumo

Desde que o resto da divisão de um inteiro positivo $n \geq 3$ por um inteiro $d > 0$ fica limitado por 0 e $d - 1$, podemos estabelecer uma correspondência biunívoca entre o conjunto das classes residuais módulo n e o conjunto das raízes de ordem n da unidade complexa. Dado que cada uma dessas raízes representa um vértice de um polígono regular, temos, por isomorfismo, que o conjunto desses pontos do plano, aditivamente, é uma cópia do conjunto $\mathbb{Z}_n$.

Palavras chave: Conjuntos, operações, isomorfismos e polígonos.

Abstract

Since the remainder of the division of a positive integer $n \geq 3$ by an integer $d > 0$ is bounded by 0 and $d - 1$, can establish a biunivocal correspondence between the set of residue classes module n and the set of order n roots of complex unit . Given that each of these roots is a vertex of a regular polygon, we have, by isomorphism, that all of these points in the plane, additively, is a copy of the set $\mathbb{Z}_n$.

Keywords: Sets, operations, isomorphism and polygons.

Lista de Símbolos

$<$: menor que,

$>$: maior que

$\leq$: menor ou igual que

$\geq$: maior ou igual que

$\neq$: diferente

$\cong$: isomorfo a

$\forall$: para todo, qualquer que seja

$\Rightarrow$: então, implica

$\Leftrightarrow$: equivalente, se e somente se, se e só se

$/$: tal que

$\exists$: existe

$\nexists$: não existe

$\in$: pertence a

$\notin$: não pertence a

$\subset$: está contido,

$\not\subset$: não está contido.

$\cup$: união $\cap$: interseção

$\mathbb{N}$: Conjunto dos números naturais

$\mathbb{Z}$: Conjunto dos números inteiros

$\mathbb{Q}$: Conjunto dos números racionais

$\mathbb{R}$: Conjunto dos números reais

$\mathbb{C}$: Conjunto dos números complexos

$\mathbb{U}_n$: Conjunto das raízes enésimas da unidade (n>2)

D(δ): Domínio da função δ

CD(δ): Contra - Domínio da função δ

Sumário

Introdução

Os conteúdos que compõem a grade curricular do mestrado profissional em matemática – PROFMAT/SBM permitem uma satisfatória atualização de nossos conhecimentos sobre Funções, Geometria, Geometria Analítica, Aritmética e Álgebra, permitindo, inclusive, que aprendamos a relacionar vários assuntos e conceitos já estabelecidos nessa parte da Matemática.

Um importante resultado que envolve os números inteiros e o conceito de divisão é o algoritmo da divisão euclidiana: para quaisquer dois inteiros a e b, com $a \neq 0$, sempre existem dois únicos inteiros q e r, tais que $b = qa + r$ e $0 \leq r < |a|$.

A divisão está presente desde cedo em diversas atividades cotidianas das crianças, como dividir objetos com um colega, repartir quantidades em partes iguais, colocar uma mesma quantidade de objetos em diversos recipientes (*LAUTERT; SPINILLO, 2002*).

Nessa fase de consolidação do conhecimento da criança, existe uma preocupação maior em compreender e efetuar a operação de divisão do que com o fato de que o quociente (ou resultado dessa operação) e o resto de uma divisão sejam únicos. E, claro, nessa fase, a unicidade desses números inteiros que surgem ao efetuarmos uma divisão podem ficar em segundo plano.

O estudo das funções em conjunto com as estruturas algébricas permite que façamos boas comparações. Os isomorfismos entre os espaços vetoriais, que estudamos na Álgebra Linear, são particulares exemplos de como podemos associar os aspectos algébricos de duas estruturas. Por exemplo, partindo de uma definição de multiplicação entre pontos (ou vetores) do plano, podemos definir um homomorfismo bijetor do conjunto $\mathbb{C}$ dos números complexos para $\mathbb{R}^2$, que é uma forma concreta de apresentarmos esses números.

Esse é um dos pontos de partida para a comparação entre duas estruturas que queremos fazer. Vamos, a partir das raízes de ordem n da unidade complexa, determinar um polígono regular de n lados e, através de um isomorfismo, mostrar que o conjunto dos vértices desse polígono pode ser identificado como o conjunto das classes de equivalência módulo n, este inteiro. As noções da teoria dos

conjuntos, o emprego do Algoritmo da divisão de Euclides, propriedades do Máximo Diviso Comum e as descrições do conjunto dos números complexos, além da identificação das raízes da unidade como sendo vértices de um polígono regular, nos convidam a fazer uma leitura agradável e complementar, no sentido de que os conteúdos estão organizados e rigorosamente de acordo com a linguagem matemática e podem servir de material de apoio para professores estudantes de matemática.

No primeiro capítulo serão apresentadas as fundamentações para o trabalho. Os conceitos da Teoria dos Conjuntos englobam operações e suas propriedades e as relações de equivalência, onde destacamos a relação de congruência modulo um inteiro n. As noções de Aritmética nos permitem concluir que o conjunto quociente de $\mathbb{Z}$ por $\equiv (mod\ n)$, definido por $\mathbb{Z}/_{\equiv (mod\ n)} = \mathbb{Z}_n = \{\bar{z}/z \in \mathbb{Z}\}$, contém exatamente n elementos e que nele podemos definir operações de adição e multiplicação. Nesse contexto, o Algoritmo da Divisão Euclidiana é decisivo. Depois de darmos uma descrição do conjunto dos números complexos, ao final do capítulo, utilizando o conceito de homomorfismo, mostramos que $\mathbb{C}$ é isomorfo ao plano $\mathbb{R}^2$ e apresentamos formas "mais concretas" de um número complexo.

No segundo capítulo, será exibido o passo a passo da construção de alguns polígonos regulares inscritos em uma circunferência. As construções que podem ser feitas por meio de régua e compasso, foram efetuadas por meio do Geogebra (software de matemática dinâmica que combina conceitos de geometria, álgebra e cálculo.). Discutimos, ainda, a construção dos polígonos regulares de 7, 9 e 27 lados. Depois de estabelecermos que as raízes complexas da unidade possam ser vistas como os vértices de um polígono regular, inscrito em uma circunferência de raio 1, nos convencemos que essa é uma forma mais precisa de construção daqueles polígonos impossíveis de serem construídos através de régua e compasso, de acordo com o **Teorema de Gauss-Wantzel**.

Através da fórmula de De Moivre, calculamos as potências das raízes de ordem n de alguns números complexos, no intuito de mostrar que, em geral, o conjunto desses pontos do plano não é fechado para a multiplicação. Dessa forma,

deixamos claro o porquê de nossas considerações recaírem sobre o conjunto $\mathbb{U}_n$, das raízes de ordem n da unidade complexa.

No último parágrafo, será feito um estudo da estrutura multiplicativa do conjunto das raízes de ordem n da unidade, comparando-a, através de um isomorfismo, com a estrutura aditiva do conjunto das classes de congruência módulo n.

Segundo Ian Stewart em [1], *"Somar é muito mais simples que multiplicar"*. Isso se contrapõe a uma ideia muito difundida por René Descartes [2], *"Não existem métodos fáceis para resolver problemas difíceis"*.

Embora, o contexto desses pontos de vista tenha sido em relação à importância do estudo dos logaritmos, cujos cálculos em produtos são facilitados por meio de uma "transformação" em soma de cálculos de logaritmos, as nossas discussões têm o mesmo sentido, quando nos propomos a estudar propriedades relacionadas a uma estrutura algébrica multiplicativa, através de propriedades observadas em uma estrutura algébrica aditiva. Nós encerramos as nossas discussões mostrando que todas as propriedades da estrutura multiplicativa do conjunto $\mathbb{C}$, valem para o conjunto $\mathbb{U}_n$.

Capítulo 1 – Conceitos Preliminares e Fundamentações

Nosso primeiro capítulo trata essencialmente das propriedades de uma operação definida em um conjunto não vazio. As relações de equivalência definidas no parágrafo 2 é uma das chaves para a conexão que faremos entre objetos geométricos e algébricos, parte central de nosso trabalho.

§1.1 Noções da Teoria dos Conjuntos

Neste parágrafo estabeleceremos o conceito de conjunto e elemento de um conjunto e abordamos algumas noções básicas e gerais da teoria dos conjuntos, enfatizando operações e propriedades. Particularmente, incluímos o conjunto dos números complexos sobre o qual também recaem as nossas principais observações.

1.1.1 Definições:

a) Denominamos de *conjunto* toda e qualquer coleção de objetos (inclusive uma coleção sem objetos).

b) Cada objeto de um conjunto será chamado de *elemento*.

Quase sempre representaremos um conjunto por uma letra maiúscula do nosso alfabeto, colocando os seus elementos entre chaves. E por letras minúsculas de nosso alfabeto representaremos os elementos de um conjunto.

Se a é um elemento do conjunto A, dizemos que "*a pertence ao conjunto A*" e anotamos isso por: $a \in A$. Caso contrário, se "*a não pertence ao conjunto A*", anotaremos: $a \notin A$.

Sejam A e B conjuntos. Se todo elemento de A, é também elemento de B, dizemos que "*A está contido em B*" e anotamos $A \subset B$. Caso contrário, se pelo menos um elemento de A não está contido em B, anotamos $A \not\subset B$, que significa que "*A não está contido em B*".

Admitimos que, para qualquer objeto ou elemento x e um conjunto A dados, ocorra exatamente uma das duas possibilidades, ou $x \notin A$ ou $x \in A$. Além disso, se os elementos a_1 e a_2 estão em A, temos como verdadeira somente uma das duas possibilidades: $a_1 = a_2$ ou $a_1 \neq a_2$.

1.1.2 Definição: Dois conjuntos A e B são *iguais* se, e somente se, A e B possuem os mesmos elementos ou se, e somente se, $A \subset B$ e $B \subset A$.

A igualdade de conjuntos representa um dos axiomas básicos da teoria axiomática de ZFC (**Zermelo-Fraenkel-Choise**). O ***Axioma da Extensionalidade:*** *Se cada elemento de A é um elemento de B e cada elemento de B representa um elemento de A, então $A = B$.*

A existência do conjunto vazio é também um dos axiomas básicos dessa teoria. O ***Axioma da Existência:*** *Existe um conjunto, denotado por ϕ e chamado de vazio, que não possui elementos.*

1.1.3 Observação: Uma coleção sem objetos é denominada de *conjunto vazio*. Tal conjunto será denotado pela letra grega ϕ. Vale que $\phi \subset X$, para todo X imaginável.

Assim, toda lista de conjuntos tem como conjunto mais elementar o conjunto vazio. Isso é devido à definição de "*não está contido*" mencionada em um de nossos parágrafos acima. Se X é qualquer conjunto, só teríamos $\phi \not\subset X$, se existisse pelo menos um elemento $a \in \phi$, tal que $a \notin X$. Como em ϕ não existem elementos, admitiremos por falta de argumentos, que $\phi \subset X$, independentemente da natureza dos elementos desse conjunto X.

Pelos mesmos argumentos que nos indicam que devemos considerar a inclusão acima, podemos admitir a unicidade do conjunto vazio, pois se supormos que são vazios os conjuntos ϕ_1 e ϕ_2 concluiremos que $\phi_1 \subset \phi_2$e que $\phi_2 \subset \phi_1$; ou seja, que $\phi_1 = \phi_2$.

Por $\nexists A$, denotaremos a quantidade de elementos do conjunto A. Se $\nexists A = 1$, diremos que o conjunto A é unitário. O conjunto vazio tem, exatamente, $\nexists \phi = 0$ elementos.

1.1.4 Definição: Sejam A e B conjuntos. Definimos:

a) $A \cup B = \{x/x \in A$ ou $x \in B\}$ conjunto *união* de A com B.

b) $A \cap B = \{x/x \in A$ e $x \in B\}$ o conjunto *interseção* de A com B.

c) Se $A \subset \Omega$, $C_\Omega\ (A) = \{x/x \in \Omega$ e $x \notin A\}$ o *conjunto complementar* de A em relação a Ω, nesta ordem.

d) $A\backslash B = \{x/x \in A \text{ e } x \notin B\}$, o *conjunto diferença* entre A e B, nesta ordem. Claro que se tem $B \subset A$ ocorre que $A\backslash B = C_A\ (B)$.

e) $A \times B = \{(a, b)\ /a \in A \text{ e } b \in B\}$, o *produto cartesiano* entre A e B, nesta ordem.

f) $P(A) = \{X/X \subset A\}$, o conjunto formado por todos os subconjuntos de A, é denominado o *conjunto das partes* de A.

Se A possui n elementos é possível mostrar, por indução, que $P(A)$ possui 2^n; elementos $\forall\ n \in \mathbb{N}$. Isso sugere que $P(A)$ também seja chamado *conjunto potência* de A.

Olhando em um conjunto não vazio podemos definir leis de composição internas entre seus elementos, que são comumente chamadas de operações.

1.1.5 Definição: Seja A um conjunto não vazio. Dizemos que uma *operação* $*$ está (*bem*) *definida* em A se, e somente se, $\forall\ x, y \in A$ vale que $x * y \in A$.

São exemplos de operações bem definidas em um conjunto não vazio:

- a adição "+" em $\mathbb{N}$;

- a união $\cup$ em $P(A)$, sendo A um conjunto não vazio;

- a multiplicação "$\cdot$" no conjunto $M_2\ (\mathbb{R})$ das matrizes quadradas de ordem 2.

A adição "+" em $\mathbb{N}$ não está bem definida em I, o conjunto o dos números ímpares, já que a soma de dois números ímpares é um número par.

Algumas operações definidas em um conjunto não vazio A possuem certas propriedades que vamos listar a seguir.

1.1.6 Definição: Sejam A um conjunto não vazio e $*$ uma operação definida em A.

a) Dizemos que esta operação tem a *propriedade associativa* se, e somente se, $\forall\ a, b, c\ \in A$, vale que $a * (b * c) = (a * b) * c$.

b) Dizemos que esta operação tem a *propriedade comutativa* se, e somente se, $\forall\ a, b\ \in A$, vale que $a * b = b * a$.

c) Dizemos que $e \in A$ é *elemento neutro* para a operação $*$ se, e somente se, vale que $\forall\ a \in A$, vale que $a * e = e * a = a$.

d) Se a operação $*$ admite elemento neutro e, dizemos que um elemento $a \in A$ possui *inverso* com respeito à operação $*$ se, e somente se,

$$\exists\, a^{-1} \in A, \text{ tal que } a * a^{-1} = a^{-1} * a = e.$$

1.1.7 Exemplos:

a) Em $P(\Omega)$, com $\Omega = \{a, b, c\}$, as operações união e interseção estão bem definidas e admitem a propriedade comutativa, isto é, para quaisquer X, Y em $P(\Omega)$, valem as seguintes igualdades: $X \cup Y = Y \cup X$ e $X \cap Y = Y \cap X$.

b) Sejam $S = \left\{ \begin{matrix} f: \mathbb{R} \longrightarrow \mathbb{R} \\ x \mapsto f(x) = ax + b \end{matrix} \quad / a, b \in \mathbb{R}, a \neq 0 \right\}$ e " $\circ$ " a operação composição de função. Claramente, as funções f e g definidas abaixo estão em S.

$$\begin{matrix} f: \mathbb{R} \longrightarrow \mathbb{R} \\ x \mapsto f(x) = x + 3 \end{matrix} \quad \text{e} \quad \begin{matrix} g: \mathbb{R} \longrightarrow \mathbb{R} \\ x \mapsto g(x) = -x \end{matrix}$$

Agora, vale que

$g \circ f: \mathbb{R} \longrightarrow \mathbb{R}$

$$x \mapsto (g \circ f)(x) = g\big(f(x)\big) = -(x + 3) = -x - 3$$

e

$f \circ g: \mathbb{R} \longrightarrow \mathbb{R}$

$$x \mapsto (f \circ g)(x) = f\big(g(x)\big) = f(-x) = -x + 3$$

Embora $D(f) = D(g) = CD(f) = CD(g)$, temos claramente que $(f \circ g)(x) \neq (g \circ f)(x)$, o que mostra que $f \circ g \neq g \circ f$. Portanto, a operação "$\circ$" não é comutativa.

c) Considerando a adição no conjunto $\mathbb{Z}$ dos números inteiros, temos que: 0 é o elemento neutro e todo elemento possui inverso. Particularmente, temos que $7^{-1} = -7$.

d) Considerando a multiplicação no conjunto $\mathbb{Q}$ dos números racionais, temos que: 1 é elemento neutro e todo elemento não nulo possui inverso. Particularmente, temos $7^{-1} = \frac{1}{7}$.

e) Se A é um conjunto não vazio, podemos considerar $P(A)$, o conjunto das partes de A. É fácil ver que as operações ∩ (interseção) e ∪ (união) estão definidas em $P(A)$. Além disto, A e ϕ são, respectivamente, o elemento neutro de ∩ e ∪.

1.1.8 Definição: (As Leis do Cancelamento): Seja A um conjunto não vazio e $*$ uma operação definida em A. Se para $a, b, c \in A$, temos:

$$a * b = a * c \Leftrightarrow b = c \text{ (cancelamento à esquerda)}$$

$$b * a = c * a \Leftrightarrow b = c \text{ (cancelamento à direita)},$$

dizemos que valem as *leis do cancelamento* para a operação $*$ definida em A.

1.1.9 Exemplos:

a) Do fato de que não existem divisores de zero, juntamente com o fato de que a multiplicação é comutativa no conjunto $\mathbb{Z}$ dos números inteiros, podemos verificar que as leis do cancelamento valem quase sempre para a multiplicação nesse conjunto: $\forall\, x, y, z \in \mathbb{Z}$, com $x \neq 0$, vale que $xy = yx = xz = zx \Leftrightarrow y = z$.

b) Seja A um conjunto não vazio e $P(A) = \{X / X \subset A\}$ o conjunto das partes de A. Claramente a interseção "∩" está bem definida em $P(A)$. Mas, para os conjuntos A, B, C em $P(A)$ com $A \cap B = A \cap C$, em geral, não vale que $A = B$.

1.1.10 Observação: O elemento neutro e inverso, relativo a uma dada operação $*$ definida em um conjunto A não vazio, quando existem, são únicos.

Demonstração: Primeiramente, suponhamos que e seja o elemento neutro para a operação $*$ definida em A. Então, para todo $a \in A$, vale que $a * e = e * a = a$. Agora, se para $e' \in A$, também vale que $a * e' = e' * a = a$, vemos que $e = e' * e = e * e' = e'$, o que prova a unicidade de e em A. ∎

A unicidade do elemento inverso é provada de maneira semelhante.

1.1.11 Definição (Potências inteiras): Seja A um conjunto não vazio, "$*$" uma operação bem definida em A e e o elemento neutro para essa operação. Então, definimos as *potências inteiras* para um elemento a em A, da seguinte maneira:

$a^0 = e$

$a^1 = a$

$a^2 = a * a$

$a^3 = a * a * a$

.....

$a^n = \underbrace{a * a * \ldots * a}_{n \text{ vezes}}$

$a^{-n} = (a^{-1})^n = \underbrace{a^{-1} * a^{-1} * \ldots * a^{-1}}_{n \text{ vezes}}$, se existir a^{-1}, o inverso de a com respeito à operação $*$.

1.1.12 Definição: Se os elementos de A podem ser operados com os elementos de B, via uma operação $*$, A e B conjuntos não vazios, então, podemos construir o conjunto $A * B = \{a * b / a \in A \text{ e } b \in B\}$.

1.1.13 Exemplos:

a) Calculando algumas potências de 5, em relação à operação de adição em $\mathbb{Z}$, obtemos

$5^0 = 0,$

$5^1 = 5,$

$5^2 = 5 + 5 = 10,$

.....

$5^n = 5 + 5 + \ldots + 5 = 5n.$

$5^{-1} = -5,$

$5^{-2} = -5 + (-5) = -10,$

.....

$5^{-n} = -5 + (-5) + \ldots + (-5) = n(-5) = -5n.$

b) Dados $M = \{1, 2, 3, 5, 7, 11\}$ e $N = \{2, 4, 6, 8\}$, podemos calcular os seguintes conjuntos:

$$M + N = \{m + n / m \in M \text{ e } n \in N\} = \{3, 4, 5, 6, 7, 8, 9, 10, 11, 13, 15, 17, 19\}$$

e

$$M - N = \{-7, -6, -5, -4, -3, -2, -1, 0, 1, 3, 5, 7, 9\}$$

Notemos que

$$M - N \neq M \backslash N = \{1, 3, 5, 7, 11\}$$

1.1.14 Definições:

a) Dizemos que dois *conjuntos* A e B são *disjuntos* se, e somente se, a intersecção entre eles é o conjunto vazio.

b) Uma *partição* de um conjunto $S \neq \phi$, é toda coleção $\mathcal{C}$ de subconjuntos de S tal que, obedece as seguintes condições:

i) $X \neq \phi$; $\forall\, X \in \mathcal{C}$;

ii) $X \cap Y = \phi$; $\forall\, X, Y \in \mathcal{C}$, com $X \neq Y$;

iii) $\bigcup_{L \in \mathcal{C}} L = S$.

1.1.15 Exemplos:

a) Todo conjunto unitário $A = \{a\}$ tem exatamente uma partição: $\{\{a\}\}$;

b) Sendo $2\mathbb{Z}$ e I os conjuntos dos números pares e ímpares, respectivamente, temos que $\{2\mathbb{Z}$, I$\}$ é uma partição de $\mathbb{Z}$.

c) Denominando $\bar{0}$, $\bar{1}$ e $\bar{2}$, os conjuntos dos números inteiros que divididos por 3 deixam restos 0, 1 e 2, respectivamente, temos também que $\{\bar{0}, \bar{1}, \bar{2}\}$ é uma partição de $\mathbb{Z}$.

Uma partição especial de um conjunto pode ser obtida a partir de uma relação de equivalência. Esse tipo de relação, que iremos definir a seguir, pode ser de fundamental importância para a compreensão da estrutura do conjunto sobre o qual ela venha a estar definida.

1.1.16 Definição: Uma relação $\sim$ sobre um conjunto A não vazio é chamada de *relação de equivalência* se, e somente se, $\forall\, a, b, c \in A$,

i) $a \sim a$ (o que significa dizer que $\sim$ é reflexiva);

ii) Se $a \sim b$; então $b \sim a$ (o que significa dizer que $\sim$ é simétrica);

iii) Se $a \sim b$ e $b \sim c$; então $a \sim c$ (o que significa dizer que $\sim$ é transitiva).

1.1.17 Exemplos:

a) A relação $=$ de igualdade em $\mathbb{R}$: $x \sim y \Leftrightarrow x = y$ é uma relação de equivalência.

b) Em $\mathbb{N}$, a relação: $x \sim y \Leftrightarrow$ x e y deixam o mesmo resto quando divididos por 5 é reflexiva, simétrica e transitiva.

c) A relação $\equiv$ de congruência no plano euclidiano: $T_1 \sim T_2 \Leftrightarrow T_1 \equiv T_2$ é tal que: $\forall\, T_1, T_2, T_3$ triângulos sobre o plano, valem:

i) $T_1 \equiv T_1$;

ii) se $T_1 \equiv T_2$; então, $T_2 \equiv T_1$;

iii) se $T_1 \equiv T_2$ e $T_2 \equiv T_3$; então, temos $T_1 \equiv T_3$.

d) Seja A o conjunto dos dias do mês de Maio do ano de 2015. Definindo que: para quaisquer dias d_1 e d_2 do mês de maio, $d_1 \sim d_2 \Leftrightarrow d_1$ e d_2 caem no mesmo dia da semana, vale que $\sim$ é uma relação de equivalência.

Domingo	Segunda	Terça	Quarta	Quinta	Sexta	Sábado
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24/31	25	26	27	28	29	30

Nesse caso, temos claramente que o dia 28 não se relaciona com o dia 10 de maio, enquanto que 4, 11 e 25 se relacionam, caindo todos numa segunda feira.

Notemos que a relação de igualdade pode ser definida em qualquer conjunto A não vazio. Evidentemente, depois de se saber comparar os elementos desse conjunto.

Se A é o domínio de uma função f, comparando os elementos de $f(A)=Im(A)$, temos uma relação induzida por f, que pode ser visto como uma generalização da relação de igualdade do item a). Basta tomar f como sendo a função identidade em A.

1.1.18 Definição: Seja $\sim$ uma relação de equivalência definida em um conjunto A não vazio. Então o conjunto:

a) $\bar{a} = \{x \in A \ / x \sim a\}$ é denominado *classe de equivalência* do elemento a;

b) $A/_{\sim} = \{\bar{a}/a \in A\}$ é denominado *conjunto quociente* de A pela relação $\sim$.

1.1.19 Exemplos:

Olhando nos exemplos em 1.1.17, vemos que:

a) No item a), para cada $r \in \mathbb{R}$, $\bar{r} = \{r\}$ é sempre um conjunto unitário. Além disso, o conjunto quociente $\mathbb{R}/_{=}$ é um conjunto infinito.

b) No item d), temos $\overline{7} = \{7,14,21,28\}$ e $\text{Maio}/_{\sim} = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}\}$.

1.1.20 Observação: Seja $\sim$ uma relação de equivalência definida em um conjunto A não vazio. Então, as seguintes proposições são equivalentes:

i) $a \sim b$;

ii) $a \in \bar{b}$;

iii) $b \in \bar{a}$;

iv) $\bar{a} = \bar{b}$.

Demonstração: Pode ser feita no sentido i) ⇒ ii), ii) ⇒ iii), iii) ⇒ iv) e iv) ⇒ i). Menos evidente é o passo iii) ⇒ iv): Por hipótese $b \in \bar{a}$ e assim $b \sim a$. Equivalentemente, por simetria, $a \sim b$. Então, para todo $x \in \bar{a}$, vale que $x \sim a$. Por transitividade, vemos que $x \sim b$. Isso mostra que $x \in \bar{b}$ e então $\bar{a} \subset \bar{b}$. Argumentos análogos mostram que $\bar{b} \subset \bar{a}$ e, portanto, vale que a igualdade $\bar{a} = \bar{b}$.■

1.1.21 Observação: Se $\sim$ é uma relação de equivalência definida em um conjunto A não vazio; então o conjunto $A/_{\sim}$ é uma partição de A.

Demonstração: (Ver definição 1.1.14, item b). Dado que $\sim$ é reflexiva, temos sempre que $a \sim a$. Então, $a \in \bar{a}$ e por isso, vale que $\bar{a} \neq \phi$; $\forall\ \bar{a} \in A/_{\sim}$. Que toda classe $\bar{a}$ é um subconjunto de A, é claro.

Agora, $\forall\ \bar{a}, \bar{b} \in A/_{\sim}$, se $\bar{a} \cap \bar{b} \neq \phi$, existe um elemento $x \in \bar{a} \cap \bar{b}$, e assim, $x \in \bar{a}$ e $x \in \bar{b}$. Daí, $x \sim a$ e $x \sim b$. Segue imediatamente que $a \sim b$ e, por 1.2.5, temos que $\bar{a} = \bar{b}$. Isso mostra que se $\bar{a} \neq \bar{b}$; então, de fato, vale que $\bar{a} \cap \bar{b} = \phi$.

Por fim, $\forall\ y \in \bigcup_{\bar{a} \in A/_{\sim}} \bar{a}$, para alguma classe $\bar{a}$, $y \in \bar{a} = \{x \in A\ / x \sim a\} \subset A$; ou seja, $y \in A$. Por outro lado, $\forall\ a \in A$, vale que $a \in \bar{a} = \{x \in A\ / x \sim b\} \subset \bigcup_{\bar{a} \in A/_{\sim}} \bar{a}$. Daí, temos a igualdade: $\bigcup_{\bar{a} \in A/_{\sim}} \bar{a} = A$.∎

§1.2 Uma Partição Especial do Conjunto $\mathbb{Z}$ dos Números Inteiros

Esse parágrafo é um preparo para a construção de um conjunto finito que tem a mesma estrutura aditiva do conjunto dos números inteiros.

1.2.1 O Conjunto $\mathbb{Z}$ dos Números Inteiros

O conjunto $\mathbb{Z}$ é a base da construção dos números racionais e a álgebra dos inteiros é de fundamental importância no estudo das estruturas algébricas.

No *conjunto* $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$ dos números inteiros estão definidas as operações de adição $(+)$ e multiplicação $(\cdot)$. Valem as seguintes propriedades: $\forall\ a, b, c \in \mathbb{Z}$

$\boldsymbol{A_1}$: $a + (b + c) = (a + b) + c$

$\boldsymbol{A_2}$: $a + b = b + a$

$\boldsymbol{A_3}$: $\exists\ 0 \in \mathbb{Z}$ tal que $0 + a = a + 0 = a$

$\boldsymbol{A_4}$: $\exists\ -a = (-1)a \in \mathbb{Z}$ tal que $a + (-a) = -a + a = 0$

$\boldsymbol{M_1}$: $a.(b.c) = (a.b).c$

$\boldsymbol{M_2}$: $a.b = b.a$

$\boldsymbol{M_3}$: $\exists\ 1 \in \mathbb{Z}$ tal que $1.a = a.1 = a$

$\boldsymbol{M_4}$: Se $a.b = 0$, então $a = 0$ ou $b = 0$. (Em $\mathbb{Z}$ não existem divisores de zero).

$\boldsymbol{D}$: $a.(b + c) = a.b + a.c = b.a + c.a = (b + c).a$

Além disso, usando que $0 + 0 = 0$, vemos que: $0.z = z.0 = 0; \forall\ z \in \mathbb{Z}$.

1.2.2 Definição: O número inteiro $|a| = \begin{cases} a\ se\ a \geq 0 \\ -a\ se\ a\ < 0 \end{cases}$ é denominado *valor absoluto* do número inteiro a.

Comumente, $|a|$ é chamado de módulo de a. Olhando cada ponto da reta como um número, entendemos que $|a|$ representa a distância de a até origem da reta. Assim, por exemplo, $|3| = 3 = -(-3) = |-3|$.

Consoante com a definição de $|a|$, para todo inteiro a, temos: $|a| \geq 0,\ |a|^2 = a^2, |-a| = |a|,\ a \leq |a|$.

O valor absoluto de um número inteiro a também pode ser definido pelas igualdades: $|a| = máx(-a, a) = \sqrt{a^2}$; onde $\sqrt{a^2}$ denotada a raiz quadrada (não negativa) de a^2 e $máx(-a, a)$ indica o maior dos inteiros $-a$ e a. Dessa forma, $|-2| = \sqrt{(-2)^2} = -(-2) = máx(2, -2)$.

De fácil verificação são os itens seguintes:

1.2.3 Observação: Se a e b são dois inteiros, então valem:

a) $|a.b| = |a|.|b|$;

b) $|a + b| \leq |a| + |b|$;

c) $|a - b| \leq |a| + |b|$.

Demonstração: a) pela definição de módulo, temos $|a.b| = \sqrt{(a.b)^2} = \sqrt{a^2.b^2} = \sqrt{a^2}.\sqrt{b^2} = |a|.|b|$.

b) temos $-|a| \leq a \leq |a|$ e $-|b| \leq b \leq |b|$. Somando ordenadamente estas desigualdades, obtemos $-(|a| + |b|) \leq a + b \leq |a| + |b|$, o que implica que $|a + b| \leq |a| + |b|$.

c) pelo item b) e como – b = +(–b), vale que $|a - b| = |a + (-b)| \leq |a| + |-b| = |a| + |b|$.∎

1.2.4 Observação: Seja S um subconjunto de $\mathbb{Z}$ ($S \subset \mathbb{Z}$). Suponhamos que $1 \in S$ e que $z.s \in S$ para todo $s \in S$ e todo $z \in \mathbb{Z}$. Então, $S = \mathbb{Z}$.

Demonstração: Temos que $S \subset \mathbb{Z}$. Então, devemos mostrar que $\mathbb{Z} \subset S$. Sabemos que para todo $z \in \mathbb{Z}$ e todo $s \in S$, temos $z.s \in S$. Fazendo $s = 1$, já que $1 \in$ S, segue que $z.1 = z \in S$. Como z é um elemento qualquer de $\mathbb{Z}$, vemos que $\mathbb{Z} \subset S$. Portanto, concluímos que $S = \mathbb{Z}$.∎

1.2.5 Definição: Dados dois números inteiros a e b, diremos que a divide b, escrevendo a \ b, quando existir c $\in \mathbb{Z}$ tal que b = ca. Neste caso, diremos também que a é um divisor ou um fator de b ou, ainda, que b é um múltiplo de a.

1.2.6 Observação (Propriedade Arquimediana em $\mathbb{Z}$): Se $a, b \in \mathbb{Z}$ e $b \neq 0$, então existe $n \in \mathbb{Z}$ tal que $nb > a$.

Demonstração: Como $|b| > 0$, temos $|b| \geq 1$ e $(|a| + 1)|b| > |a| + 1 > |a| > a$. Assim, se $b > 0$, basta tomarmos $n = |a| + 1$. Se $b < 0, n = -(|a| + 1)$. Isso termina a demonstração.∎

Além dessa propriedade, usaremos o Princípio da Boa Ordenação - P.B.O. (ver [4]; pág. 16) para provarmos, devido a Euclides, a importante observação que segue.

1.2.7 Observação (Divisão Euclidiana): Sejam a e b números inteiros com $a \neq 0$. Então, existem únicos inteiros q e r de modo que $b = aq + r$; com $0 \leq r < |a|$.

Demonstração: Considere o conjunto $S = \{0 \leq b - ay / \ y \in \mathbb{Z}\}$. Por 1.2.6, existe um inteiro $n \in \mathbb{Z}$ tal que $b - ny > 0$. Isso mostra que $S \neq \phi$. Pelo P.B.O., S possui um primeiro elemento; digamos, $r = b - aq \geq 0$.

Agora, se temos $r \geq |a|$, vale que $r = |a| + s$ e assim, temos $0 \leq s < r$; já que $a \neq 0$ e $|a| > 0$. Mas, então $s = r - |a| = (b - aq) - |a| = b - (q \pm 1)a \in S$. Uma contradição com a escolha do r. Portanto, temos $0 \leq r < |a|$ e $b = aq + r$.

Para provar a unicidade dos inteiros q e r podemos supor que $b = aq + r = aq' + r'$ e, usando as desigualdades $0 \leq r < |a|$ e $0 \leq r' < |a|$, concluir que $a = a'$ e, consequentemente, que $r = r'$ (ver [4]; pág. 17) .∎

1.2.8 Definição: Sejam a e b números inteiros quaisquer e seja n > 1 um inteiro fixo. Dizemos que a é congruente a b módulo n se, e somente se, n divide a diferença a $-$ b ou seja existe um inteiro k tal que a $-$ b $= k$n.

Escrevemos a $\equiv$ b(mod n) sempre que a é congruente a b módulo n.

De acordo com a definição em 1.1.16, é de fácil verificação que a congruência módulo n é uma relação de equivalência no conjunto $\mathbb{Z}$ dos números inteiros, comumente denotada por: $\equiv$ (mod n).

A classe de equivalência de um elemento $z \in \mathbb{Z}$, por definição, é o conjunto:

$$\bar{z} = \{x \in \mathbb{Z}/\ x \equiv z(mod\ n)\} = \{x \in \mathbb{Z}/x - z = kn; \text{com } k \in \mathbb{Z}\}$$

O conjunto quociente de $\mathbb{Z}$ por $\equiv (mod\ n)$ é, por definição, o conjunto:

$$\mathbb{Z}/_{\equiv (mod\ n)} = \{\bar{z}/z \in \mathbb{Z}\}$$

Observemos que, pondo $n\mathbb{Z} = \{nk;\ \text{com } k \in \mathbb{Z}\} = \{\cdots, -2n, -n, 0, n, 2n \cdots\}$, correspondendo ao conjunto dos múltiplos de n, podemos fazer a seguinte leitura da relação de congruência definida acima: $a \equiv b(mod\ n)$ se, e somente se, $a - b \in n\mathbb{Z}$. Dessa forma, é razoável que podemos escrever $\mathbb{Z}/_{n\mathbb{Z}}$, ao invés de $\mathbb{Z}/_{\equiv (mod\ n)}$, para denotar o conjunto quociente de $\mathbb{Z}$ por $\equiv (mod\ n)$.

De modo mais frugal ainda, adotaremos a notação $\mathbb{Z}/_{n\mathbb{Z}} = \mathbb{Z}_n$ para denotar o conjunto quociente de $\mathbb{Z}$ por $\equiv (mod\ n)$.

Sempre que nos referirmos à congruência módulo n, estaremos considerando $1 < n \in \mathbb{Z}$.

1.2.9 Observação: Para qualquer inteiro n >1, vale que $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$ possui exatamente n elementos.

Demonstração: Evidentemente, cada elemento $\bar{x}$ do conjunto $\{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$ é um elemento de $\mathbb{Z}_n$. A outra inclusão, menos evidente, pode ser mostrada da seguinte forma: $\forall\ \bar{z} \in \mathbb{Z}_n$, vale, dividindo z por n, conforme a observação em 1.2.7, que existem únicos inteiros q e r tais que $z = qn + r$, com $0 \leq r < n$. Como r é um número inteiro, vale que $r \in \{0, 1, \ldots, n-1\}$. Além disso, a igualdade $z - r = qn$ nos dá que $z \equiv r(mod\ n)$. Por 1.1.20, temos que $\bar{z} = \bar{r} \in \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$. Por 1.1.21, $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$ possui exatamente n elementos.∎

Essa pequena observação mostra que $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$ é uma partição de $\mathbb{Z}$. Ela tem um caráter especial porque nos permite construir um conjunto finito no qual, por conta do resultado em 1.1.20, podemos definir operações de adição e multiplicação. Isso será explicado no parágrafo seguinte.

§1.3 Conjuntos Aditivamente e Multiplicativamente Fechados

1.3.1 Definição: Dizemos que um conjunto $S \neq \phi$ é *fechado* para a operação $*$ ou que $*$ é uma operação *(bem) definida* em S se, e só se, $\forall\, a, b \in S$, vale que $a * b \in S$.

O conjunto dos números Irracionais não é fechado para a multiplicação pois, o produto $\sqrt{2}.\sqrt{2} = \sqrt{4} = 2 \in \mathbb{Q}$.

O fechamento de uma operação nos dá a segurança de que, ao operarmos com os objetos de um conjunto, o resultado não sairá desse conjunto.

Pode ser que não consigamos um adjetivo para os mais variados conjuntos e suas variadas operações. Mas, se a operação é de adição ou multiplicação, é comum dizermos que o conjunto é aditivamente ou multiplicativamente fechado, respectivamente.

Voltemos à relação de equivalência definida sobre $\mathbb{Z}$, a congruência módulo n descrita em 1.2.8.

1.3.2 Observação: Sejam a, b, c, d e $1 < n \in \mathbb{Z}$. Então, se $a \equiv b(mod\ n)$ e $c \equiv d(mod\ n)$ vale que:

a) $a + c \equiv b + d(mod\ n)$;

b) $ac \equiv bd(mod\ n)$.

Demonstração: Imediata (ver [5]; Unidade 18, pág. 3).∎

Claro que, além dessas igualdades, por 1.1.20, sempre temos $\bar{a} = \bar{b}$ e $\bar{c} = \bar{d}$.

Essas duas propriedades mostram que podemos definir uma adição e uma multiplicação em $\mathbb{Z}_n$.

1.3.3 Definição: Sejam $1 < n \in \mathbb{Z}$ e $\bar{a}$ e $\bar{b}$ quaisquer elementos em $\mathbb{Z}_n$. Podemos definir e estão bem definidas as seguintes operações:

$+: \bar{a} + \bar{b} = \overline{a+b}$ (adição);

$\cdot : \bar{a}.\bar{b} = \overline{a.b}$ (multiplicação).

Notemos que, devido à observação anterior, independente do representante de cada classe, essa soma ou produto das classes podem ser obtidos, simplesmente, pela classe da soma ou produto.

Se o inteiro fixado é "pequeno" podemos pensar em uma tabela que nos mostra os resultados quando somamos ou multiplicamos quaisquer dois elementos de $\mathbb{Z}_n$. Vejamos alguns exemplos.

Para $\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$, temos as tabelas:

$+$	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$

.	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$

Para $\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$, temos as tabelas:

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

.	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

A leitura dessas tabelas, comumente chamadas tábua de adição e tábua de multiplicação, deve ser feita olhando da esquerda para a direita e de cima para baixo. No cruzamento dessas filas está o resultado da adição ou da multiplicação entre os elementos das extremidades.

Depois dos argumentos acima, mesmo que destaquemos, e é importante que façamos isso, se $1 < n \in \mathbb{Z}$, temos, com relação às operações definidas em 1.3.3, que $\mathbb{Z}_n$, o conjunto quociente de $\mathbb{Z}$ pela relação $\equiv (mod\ n)$, é aditivamente e multiplicativamente fechado.

1.3.4 Observação: Para todos $\bar{a}$, $\bar{b}$ e $\bar{c} \in \mathbb{Z}_n$, com $1 < n \in \mathbb{Z}$, valem, e são de fácil verificação, as seguintes propriedades:

− Associatividade: $(\bar{a} + \bar{b}) + \bar{c} = \bar{a} + (\bar{b} + \bar{c})$ e $(\bar{a}.\bar{b}).\bar{c} = \bar{a}.(\bar{b}.\bar{c})$;

− Comutatividade: $\bar{a} + \bar{b} = \bar{b} + \bar{a}$ e $\bar{a}.\bar{b} = \bar{b}.\bar{a}$;

− Existência de elemento neutro: $\bar{a} + \bar{0} = \bar{a}$ e $\bar{a}.\bar{1} = \bar{a}$;

− Existência de inverso aditivo: $\exists\ \overline{-a} \in \mathbb{Z}_n$ tal que $\bar{a} + \overline{(-a)} = \bar{0}$.

− Distributividade da multiplicação em relação à adição: $\bar{a}.(\bar{b} + \bar{c}) = \bar{a}.\bar{b} + \bar{a}.\bar{c}$.

Claro que, "debaixo da barra", estamos relacionando tão somente as propriedades da adição e da multiplicação do conjunto $\mathbb{Z}$ dos números inteiros.

De acordo com a definição em 1.1.6, um elemento $\bar{a}$ em $\mathbb{Z}_n$ tem inverso (multiplicativo), quando existir $\bar{b} \in \mathbb{Z}_n$ tal que $\bar{a}.\bar{b} = \bar{1}$. A lista de propriedades acima já denuncia que, em relação à multiplicação que definimos em $\mathbb{Z}_n$ nem todo elemento possui inverso. A tabela de multiplicação de $\mathbb{Z}_4$, após a definição em 1.3.2, mostra que, por exemplo, além de $\bar{0}$, o elemento $\bar{2}$ não é inversível. Além disso, mostra que $\bar{2}.\bar{2} = \bar{4} = \bar{0}$, o que significa que existem divisores de zero em $\mathbb{Z}_4$.

A definição de divisibilidade em 1.2.5 e o conceito de máximo divisor comum podem ser utilizados para mostrar que, quando n é um número primo, a operação de multiplicação definida em $\mathbb{Z}_n$, em 1.3.3, possui mais propriedades.

1.3.5 Observação: Seja $1 < n \in \mathbb{Z}$ e seja $\bar{0} \neq \bar{a} \in \mathbb{Z}_n$. Então, vale que $\bar{a}$ é inversível se, e somente se, a e n são relativamente primos. Consequentemente, $\bar{a}.\bar{b} = \bar{0}$, se, e somente se, $\bar{a} = \bar{0}$ ou $\bar{b} = \bar{0}$.

Demonstração: Se $\bar{a}$ é inversível, então existe $\bar{b} \in \mathbb{Z}_n$ tal que $\bar{a}.\bar{b} = \overline{ab} = \bar{1}$, ou seja, $ab \equiv 1(mod\ n) \Leftrightarrow ab - 1 = kn \Leftrightarrow ab + (-k)n = 1$. Claro que, assim, se $0 < d$ é um divisor comum de a e n, então, vale que $d = 1$ e, por isso, a e n são relativamente primos.

Reciprocamente, se a e n são relativamente primos, existem inteiros b e t tais que $ab + tn = 1$ (ver [4]; pág. 24). Dessa igualdade concluímos que $\overline{a.b + n.t} = \bar{1} \Leftrightarrow \overline{a.b} + \overline{n.t} = \bar{1} \Leftrightarrow \overline{a.b} + \bar{0} = \bar{1} \Leftrightarrow \overline{a.b} = \bar{1}$. Portanto, $\bar{a}$ é inversível.■

Os fatos geométricos ligados ao conjunto $\mathbb{C}$ dos números complexos, que iremos descrever no capítulo 2, têm uma conexão com a estrutura do conjunto $\mathbb{Z}_n$, se $2 < n \in \mathbb{Z}$. Tal conexão, que queremos estabelecer, depende também da descrição que faremos a seguir do conjunto $\mathbb{C}$.

1.3.6 O Conjunto $\mathbb{C}$ dos Números Complexos

As definições sobre números complexos tiveram um desenvolvimento gradativo. Começaram a ser utilizados formalmente no século XVI em fórmulas de resolução de equações de graus 3 e 4.

Os primeiros que conseguiram formalizar respostas a essas equações de grau 3 foram Scipione del Ferro e Tartaglia. Fato que poderia unir duas grandes mentes matemáticas criou o oposto. Tartaglia passou seus resultado a Cardano com a promessa de não divulgá-los, contudo após verificar a exatidão das resoluções de Tartaglia, Cardano não honra sua promessa e publica os resultados, com uma menção ao autor, em sua obra Ars Magna de 1545, iniciando uma enorme inimizade.

A fórmula deduzida por Tartaglia afirmava que a solução da equação $x^3 + px + q = 0$ era função dos coeficientes p e q e podia ser expressa por $x = \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}$.

Um problema preocupante notado na época foi que algumas equações levavam a raízes quadradas de números negativos. Por exemplo, a equação: $x^3 - 15x - 4 = 0$ tem três raízes reais, o que dá pra ver se a escrevermos na forma $(x-4)(x^2+4x+1) = 0$. Assim, vemos que $x = 4$ ou $x = -2 - \sqrt{3}$ ou $x = -2 + \sqrt{3}$. Agora, usando a fórmula de Tartaglia, temos $x = \sqrt[3]{2 + \sqrt{-121}} + \sqrt[3]{2 - \sqrt{-121}}$, o que evidenciou a conjuntura de que havia mais a se pesquisar e conhecer sobre esses números.

Rafael Bombelli tentou colocar as expressões $\sqrt[3]{2 + \sqrt{-121}}$ e $\sqrt[3]{2 - \sqrt{-121}}$ na forma $a + \sqrt{-b}$ e $a - \sqrt{-b}$, respectivamente. Admitindo a validade das propriedades usuais das operações tais como distributiva, comutativa, etc., usou-as nas expressões obtidas, obtendo $a = 2$ e $b = 1$. Com isso, conseguiu chegar ao valor de $x = \sqrt[3]{2 + \sqrt{-121}} + \sqrt[3]{2 - \sqrt{-121}} = \left(2 + \sqrt{-1}\right) + \left(2 - \sqrt{-1}\right) = 4$.

A princípio, os números complexos não foram observados como números, mas sim como um artifício algébrico muito útil para a resolução de equações. No século XVII, foram chamados de *números imaginários,* denotação atribuída a Descartes. Euler e Abraham de Moivre começaram a estabelecer uma estrutura algébrica para os números complexos no século seguinte. Particularmente, Euler denotou por i a raiz quadrada de -1. Ainda neste século os números complexos começaram a ser analisados como pontos do plano (plano de Argand-Gauss), permitindo a escrita de um número complexo através da forma polar. Com isso, conseguiu-se calcular as potências e as raízes de modo eficiente e claro.

O conjunto $\mathbb{C} = \{x + yi\ /x, y \in \mathbb{R} \text{ e } i = \sqrt{-1}, \text{onde } i^2 = -1\}$ é definido como sendo o *conjunto dos números complexos*.

Claramente, o fato de que podemos escrever $r = r + 0i; \forall\ r \in \mathbb{R}$, mostra que o conjunto $\mathbb{R}$ dos números reais está contido em $\mathbb{C}$.

1.3.7 Definições: Para todo $z = x + yi \in \mathbb{C}$, definimos que:

a) o número complexo $i = 0 + i$ é a *unidade imaginária* em $\mathbb{C}$.

b) $\text{Re}(z) = x$ é a *parte real* de z.

c) $\text{Im}(z) = y$ é a *parte imaginária* de z.

d) $\bar{z} = \overline{x + yi} = x - yi$ é o *conjugado* de z.

e) (*Igualdade de números complexos*) Se $w = a + bi \in \mathbb{C}$; então vale que $z = w$, se e somente se, valerem as igualdades $\text{Re}(z) = \text{Re}(w)$ e $\text{Im}(z) = \text{Im}(w)$.

Como no conjunto dos números inteiros o módulo de um número complexo também goza de algumas propriedades relacionadas. Como algumas delas estão relacionadas com operações que podemos definir em $\mathbb{C}$, vamos primeiramente definir uma adição e uma multiplicação no conjunto dos números complexos.

1.3.8 Definição: Sejam $z = x + yi$ e $w = a + bi$ quaisquer elementos em $\mathbb{C}$. Então, podemos definir e estão bem definidas as seguintes operações:

$+: z + w = (x + yi\ ) + (a + b) = (x + a) + (y + b)i$ (adição);

$\cdot : z.w = (x + yi\ ).(a + bi) = (xa - yb) + (xb + ya)i$ (multiplicação).

Admitindo que sejam conhecidas as propriedades da adição e da multiplicação, definidas no conjunto dos números, a multiplicação, menos natural aqui, é feita com se faz a multiplicação entre somas em $\mathbb{R}$, apesar de i ser a raiz quadrada do número negativo -1. Usamos a comutatividade e a associatividade da adição e a distributiva da multiplicação em relação à adição, além de admitir que $i^2 = -1$.

1.3.9 Observação: Para quaisquer números complexos z_1, z_2 e z_3 em $\mathbb{C}$, valem e são de fácil verificação as seguintes propriedades:

$-$ Associatividade: $z_1 + (z_2 + z_3) = (z_1 + z_2) + z_3$ e $z_1\,(z_2 z_3) = (z_1 z_2) z_3$;

$-$ Comutatividade: $z_1 + z_2 = z_2 + z_1$ e $z_1 z_2 = z_2 z_1$;

$-$ Existência de elemento neutro para a adição: $\exists\ 0 = 0 + 0i \in \mathbb{C}$ tal que $0 + z_1 = z_1 + 0 = z_1$;

$-$ Existência de elemento neutro para a multiplicação: $\exists\ 1 = 1 + 0i \in \mathbb{C}$, tal que $1\ z_1 = z_1 1 = z_1$;

$-$ Existência de inverso aditivo: $\exists\ -z_1 = -a + (-b)i \in \mathbb{C}$ tal que $z_1 + (-z_1) = -z_1 + z_1 = 0$.

$-$ Existência de "muito inversos" multiplicativos: se $z_1 \neq 0, \exists\ {z_1}^{-1} \in \mathbb{C}$ tal que $z_1 {z_1}^{-1} = {z_1}^{-1} z_1 = 1 = 1 + 0i$.

$-$ Distributividade da multiplicação em relação à adição: $z_1(z_2 + z_3) = z_1 z_2 + z_1 z_3 = z_2 z_1 + z_3 z_1 = (z_2 + z_3) z_1$

Quase todas as propriedades acima podem ser mostradas tratando a unidade imaginária de $\mathbb{C}$ como se fosse também um número.

Verifiquemos a comutatividade da multiplicação: Pondo $z_1 = a + bi$ e $z_2 = c + di$, temos que $z_1 z_2 = (a + bi)(c + di) = (ac - bd) + (bc + ad)i$. Agora, $z_2 z_1 = (c + di)(a + bi) = (ca - db) + (cb + da)i$. Comparando esses produtos, depois de usar a comutatividade da adição e da multiplicação dos números, vemos que $z_2 z_1 = z_1 z_2$.

O inverso de um número complexo $z = a + bi \neq 0$ pode ser obtido pela simples resolução da equação $zw = 1$; onde $w = x + yi$ é a "variável". A igualdade de complexos revela que $z^{-1} = \frac{a}{a^2+b^2} + \left(-\frac{b}{a^2+b^2}\right) i$.

Outra propriedade que é de imediata verificação é que $0z = 0; \forall\, z \in \mathbb{C}$. Esse pequeno fato também ajuda a demonstrar a seguinte

1.3.10 Observação: Se z_1e z_2 estão em $\mathbb{C}$ e $z_1.z_2 = 0$, então temos $z_1 = 0$ ou $z_2 = 0$ (em $\mathbb{C}$ não existem divisores de zero).

Demonstração: Pelas propriedades descritas anteriormente em 1.3.9, se $z_1 \neq 0$, existe $z_1^{-1} \in \mathbb{C}$, tal que $z_1 {z_1}^{-1} = {z_1}^{-1} z_1 = 1$. Daí, vem que
$z_1.z_2 = 0 \Leftrightarrow z_1^{-1}.(z_1.z_2) = z_1^{-1}.0 \Leftrightarrow (z_1^{-1}.z_1).z_2 = 0 \Leftrightarrow 1.z_2 = 0 \Leftrightarrow z_2 = 0$. Por Argumentos análogos, se $z_2 \neq 0$, concluímos que $z_1 = 0$.■

Antes de apresentarmos uma forma mais concreta de um número complexo z, o que depende diretamente da definição de seu conjugado $\bar{z} = \overline{x + yi} = x - yi$, verificaremos algumas das principais propriedades relacionadas a esse conceito.

1.3.11 Observação: Sejam $z = x + yi$ e $w = a + bi$ quaisquer elementos em $\mathbb{C}$. Então, vale, e é de fácil verificação, que:

a) $\overline{z + w} = \bar{z} + \bar{w}$;

b) $\overline{zw} = \bar{z}\bar{w}$;

c) $\overline{-z} = -\bar{z}$;

d) se $z \neq 0 + 0i$ então $\overline{z^{-1}} = \bar{z}^{-1}$;

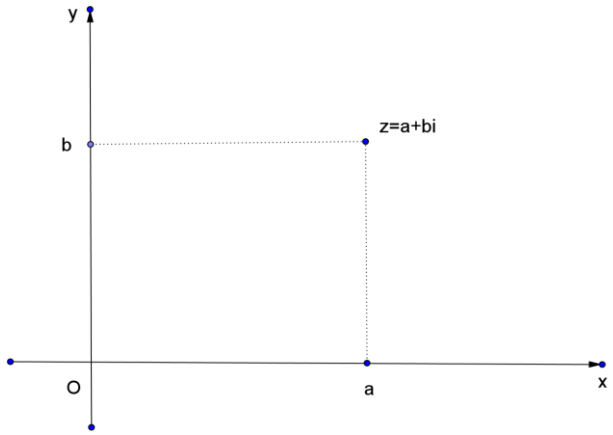
e) $z\bar{z} = x^2 + y^2$.

Demonstração: Faremos somente os itens b) e d). Temos, primeiramente, que $\overline{zw} = \overline{(x + yi)(a + bi)} = \overline{(xa - yb) + (xb + ya)i} = (xa - yb) - (xb + ya)i$. Por comparação, vemos que $\bar{z}\bar{w} = (x - yi)(a - bi) = (xa - yb) - (xb + ya)i = \overline{zw}$, o que prova d). Agora, usando o item b) e e), podemos escrever $\overline{z^{-1}}\bar{z} = \overline{z^{-1}z} = \overline{1 + 0i} = 1.\overline{1 + 0i} = (1 + 0i)\overline{1 + 0i} = 1^2 + 0^2 = 1$. Isso mostra que, de fato, $\overline{z^{-1}} = \bar{z}^{-1}$.■

Vale ressaltar que a barra, dependendo do contexto a ser analisado, pode ser a representação do conjugado de um número complexo ou a classe de equivalência de um inteiro z pela relação de congruência módulo n. Contudo, apesar da mesma representatividade, não haverá prejuízo de modo que o ambiente deixará claro sobre qual atributo estará sendo usado.

Nós podemos pensar na seguinte representação de um elemento $z = a + bi$ em $\mathbb{C}$ (ver figura abaixo): marcamos o valor de $\mathrm{Re}(z) = a$, no eixo horizontal e $\mathrm{Im}(z) = b$, no eixo vertical do plano cartesiano. Então, o encontro das retas paralelas a esses eixos e que passam por esses valores, determinam um ponto do plano que representa $z = a + bi$. O ponto (a, b) representa o número complexo $z = a + bi$ em *coordenadas cartesianas*.

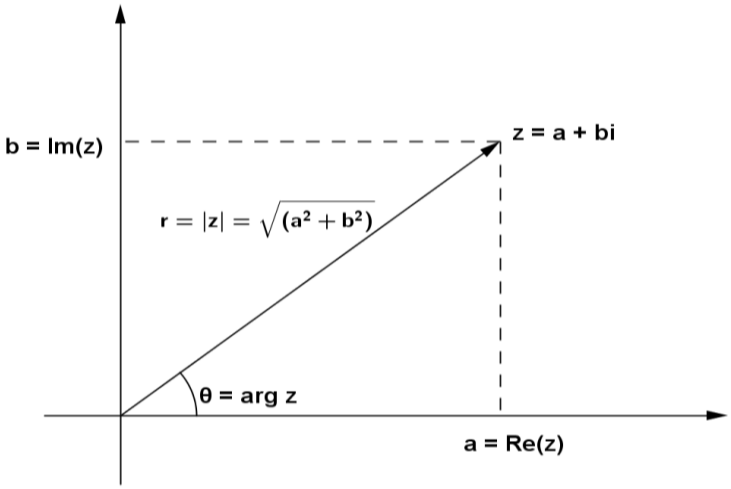
Figura 01: representação geométrica de um número complexo



Devido à definição de igualdade em 1.3.7, para cada $z = x + yi$ em $\mathbb{C}$, essa representação é única. Assim, de maneira mais concreta, podemos representar o conjunto dos números complexos como sendo $\mathbb{C} = \{(x, y)/x, \mathrm{y} \in \mathbb{R}\}$ o conjunto de pontos ou vetores de $\mathbb{R}^2$. O plano cujos pontos representam todos os elementos de $\mathbb{C}$, é chamado de *plano de Argand – Gauss*.

Agora, consideremos a figura abaixo, onde podemos desenhar um triângulo retângulo, no qual vale a relação de Pitágoras.

Figura 02: Módulo e Argumento de um número complexo



1.3.12 Definição: Na representação do número complexo $z = a + bi$ como um ponto do plano:

a) denominamos $|z| = \sqrt{a^2 + b^2}$ de *módulo do número complexo* z. Esse número não negativo é igual à distância do ponto das coordenadas cartesianas de z à origem do plano de Argand- Gauss.

b) o ângulo formado entre o segmento de reta que liga a origem $(0, 0)$ do plano ao ponto (a, b) e o eixo horizontal é chamado de *argumento do número complexo* z.

Todo número $\varphi = \theta + 2k\pi$, com $k \in \mathbb{Z}$, também é chamado de *argumento de* z. Contudo, denominamos de *argumento* (*principal*) *do número complexo z*, o único ângulo $\theta = \arg(z) \in]-\pi, \pi]$.

Ainda, no triângulo retângulo, temos $a = |z|cos\theta$ e $b = |z|sen\theta$ e assim, podemos escrever $z = a + bi = |z|(cos\theta + isen\theta)$ que é chamada a *forma trigonométrica* ou *forma polar do número complexo* z.

Para termos uma ideia de como podem ser calculadas potências de um número complexo $z = a + bi$, vamos verificar como que calculamos um produto de números complexos na forma polar.

Dados $z = |z|(cos\alpha + isen\alpha)$ e $w = |w|(cos\beta + isen\beta)$ quaisquer elementos em $\mathbb{C}$. Temos que

$$zw = \big(|z|(cos\alpha + isen\alpha)\big)\big(|w|(cos\beta + isen\beta)\big) =$$

$$|z||w|(cos\alpha cos\beta + isen\alpha cos\beta + isen\alpha cos\beta + isen\alpha isen\beta) =$$

$$|z||w|\big(cos\alpha cos\beta - sen\alpha sen\beta + i(sen\alpha cos\beta + sen\beta cos\alpha)\big) =$$

$$|z||w|\big(cos(\alpha + \beta) + isen(\alpha + \beta)\big).$$

Assim, o produto de dois números complexos na forma polar é igual a um número complexo cujo módulo é o produto dos módulos e cujo argumento é a soma dos argumentos dos números complexos multiplicados.

Usando o princípio de indução finita (ver [4]; pág. 16) e os cálculos acima, podemos verificar a validade da fórmla de De Moivre, relacionada a seguir.

1.3.13 Observação: (fórmula de De Moivre): Seja $z = |z|(cos\theta + isen\theta)$. Para todo $n \in \mathbb{N}$, vale que $z^n = |z|^n\big(cos\ (n\theta) + isen\ (n\theta)\big)$.

A demonstração desse fato pode ser feita por indução. Depois do passo indutivo os cálculos são idênticos aos que fizemos ao calcular o produto dos números complexos z e w na forma polar, nos parágrafos acima. Essencialmente, calculamos

$$z^{n+1} = zz^n = \big(|z|(cos\theta + isen\theta)\big)(|z|^n\ (cos\ (n\theta) + isen\ (n\theta))) =$$
$$|z||z|^n(cos\theta + isen\theta)(cos\ n\theta + isen\ n\theta) =$$
$$|z|^{n+1}\big(cos\theta cos(n\theta) - sen\theta sen(n\theta) + cos\theta sen(n\theta) + sen\theta icos(n\theta)\big) =$$
$$|z|^{n+1}\left(cos\big((n+1)\theta\big)\right) + i\left(sen\big((n+1)\theta\big)\right)$$

para mostrar que $\forall\ n \in \mathbb{N}$, vale a igualdade $z^n = |z|^n\big(cos\ (n\theta) + isen\ (n\theta)\big)$.

A fórmula de De Moivre se verifica para todo inteiro n. Se $n < 0$ usamos o fato de que $-n > 0$ e, por indução, concluímos, ao final, que $\forall\ n \in \mathbb{Z}$, vale a igualdade $z^n = |z|^n\big(cos\ (n\theta) + isen\ (n\theta)\big)$.

1.3.14 Observação: Consideremos o número complexo $z = |z|(cos\theta + isen\theta)$. Então, para todo $0 < n \in \mathbb{N}$, vale que $w_k = \sqrt[n]{z} = \sqrt[n]{|z|}\left(cos\,\frac{\theta+2k\pi}{n} + isen\ \frac{\theta+2k\pi}{n}\right)$; com $k = 0, 1, \cdots, n-1$, são as n raízes distintas (de ordem n) de z. Particularmente, $w_k = cos\,\frac{2k\pi}{n} + isen\ \frac{2k\pi}{n}$; com $k = 0, 1, \cdots, n-1$, são as n raízes distintas (de ordem n) da unidade $1 = 1 + 0i$ em $\mathbb{C}$.

Demonstração: Uma raiz enésima de $z = |z|(cos\theta + isen\theta)$ é um número complexo $w = |w|(cos\varphi + isen\varphi)$ tal que$w^n = z$, note que $w^n = \big(|w|(cos\varphi + isen\varphi)\big)^n = |w|^n(cos\varphi + isen\varphi)^n = |w|^n\big(cos(n\varphi) + isen(n\varphi)\big)$. Como $w = \sqrt[n]{z}$, temos que $w^n = z$; ou seja, temos $|w|^n\big(cos(n\varphi) + isen(n\varphi)\big) = |z|(cos\theta + isen\theta)$. Segue então que $|w| = \sqrt[n]{|z|}$ e $n\varphi = \theta + 2k'\pi \Leftrightarrow \varphi = \frac{\theta+2k\prime\pi}{n}$. Pondo $k' = pn + k$, com $p \in \mathbb{Z}$ e $k = 0, 1, \cdots, n-1$, temos que $\varphi = \frac{\theta+2k\prime\pi}{n} = \frac{\theta+2(pn+k)\pi}{n} = \frac{\theta}{n} + \frac{2pn\pi+2k\pi}{n} = \frac{\theta}{n} + \frac{2k\pi}{n} + 2p\pi$. Daí, entendemos que $\varphi = \frac{\theta}{n} + \frac{2k\pi}{n}$ e as n raízes de z são $w_k = \sqrt[n]{z} = \sqrt[n]{|z|}\left(cos\,\frac{\theta+2k\pi}{n} + isen\ \frac{\theta+2k\pi}{n}\right)$; com $k = 0, 1, \cdots, n-1$.∎

Notemos que, se $z = 1 + 0i = 1$, os números w_0, w_1,$\cdots$, w_{n-1} são distintos entre si, pois a diferença entre os argumentos de dois quaisquer deles não é um múltiplo de 2π. Essa diferença é igual a $\frac{2(k_1-k_2)\pi}{n}$, com k_1,$k_2 \in \{0, 1, \cdots, n-1\}$ e assim o número $\frac{(k_1-k_2)}{n}$ não é inteiro; já que $0 < \frac{(k_1-k_2)}{n} \leq \frac{n-1}{n} < 1$.

Nosso pequeno e último parágrafo deste capítulo traz o conceito de *isomorfismo* que é de fundamental importância para a identificação geométrica que queremos fazer dos elementos de $\mathbb{Z}_n$, quando fixamos $1 < n \in \mathbb{Z}$.

§ 1.4 Funções especiais: homomorfismos bijetores

Inicialmente, utilizando os conceitos aqui abordados, faremos uma "boa" identificação do conjunto $\mathbb{C}$ e, assim, mostraremos versões mais concretas do conjunto dos números complexos. No capítulo 2, efetivamente, veremos a importância dessas funções bijetivas para a problemática deste trabalho.

1.4.1 Definição: Sejam X e Y conjuntos não vazios. Suponha que $*$ é uma operação bem definida em X e que $\square$ é uma operação bem definida em Y. Uma função $\begin{matrix}\varphi : X \longrightarrow Y \\ x \mapsto \varphi(x)\end{matrix}$ é dita um *homomorfismo* se, e somente se, $\forall\, a, b \in X$, vale que $\varphi(a * b) = \varphi(a) \square \varphi(b)$.

Um homomorfismo injetivo é denominado *monomorfismo*. Se for sobrejetivo é denominado *endomorfismo*. Se for bijetivo é denominado *isomorfismo*.

1.4.1 Exemplos: Conhecemos desde cedo a função (linear) $\begin{matrix}f : \mathbb{R} \longrightarrow \mathbb{R} \\ x \mapsto f(x) = ax;\end{matrix}$ onde $0 \neq a \in \mathbb{R}$. Essa função é um homomorfismo, já que $\forall\, x, y \in \mathbb{R}$, vale que $f(x + y) = f(x) + f(y)$.

As funções reais (do Cálculo) $ln(x)$ e $exp(x)$ também são exemplos de homomorfismos. Notemos que enquanto uma leva um produto em uma soma a outra leva uma soma em um produto, respectivamente.

1.4.2 Observação: Se φ é um isomorfismo de X em Y, valem as seguintes propriedades:

a) Sejam e o elemento neutro para uma operação $*$ definida em X. e e' o elemento neutro para uma operação definida em Y. Então, se em Y valem as leis do cancelamento (lembrar 1.1.8), então $\varphi(e) = e'$.

b) Se x^{-1} é o inverso de um elemento x em X, então $\varphi(x^{-1}) = (\varphi(x))^{-1}$.

Demonstração: Primeiramente, temos que $e * e = e$. Portanto podemos escrever a igualdade $e' \square \varphi(e) = \varphi(e) = \varphi(e * e) = \varphi(e) \square \varphi(e)$; já que φ é um homomorfismo. Cancelando $\varphi(e)$ em ambos os membros da igualdade, fica demonstrado o item a).

Agora, de $x * x^{-1} = e$, obtemos $\varphi(x * x^{-1}) = \varphi(e)$. Como φ é um homomorfismo e, pelo item a), $\varphi(e) = e'$, vem que $\varphi(x) \square \varphi(x^{-1}) = e'$. Isto mostra que $\varphi(x^{-1}) = (\varphi(x))^{-1}$ e b) fica demonstrado também.∎

1.4.3 Observação: Consideremos o conjunto $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R} = \{(a, b) / a, b \in \mathbb{R}\}$. Em $\mathbb{R}^2$ podemos definir as seguintes operações: $\forall\ (a, b), (c, d) \in \mathbb{R}^2$

$+: (a, b) + (c, d) = (a + c, b + d)$

$.: (a, b).(c, d) = (ac - bd, ad + bc)$.

É fácil ver que, para essa adição e essa multiplicação definidas em $\mathbb{R}^2$, valem todas as propriedades listadas em 1.3.9.

Além disto, a função $\begin{array}{l} \delta: \mathbb{C} \longrightarrow \mathbb{R} \times \mathbb{R} \\ a + bi \mapsto \delta(a + bi) = (a, b) \end{array}$ é um isomorfismo.

Demonstração: Primeiramente, vale que: $\forall a + bi, c + di \in \mathbb{C} = D(\delta)$ se $\delta(a + bi) = \delta(c + di)$, vale que $(a, b) = (c, d) \Leftrightarrow a = c$ e $b = d$. Assim, obtemos que $a + bi = c + di$. Isto mostra que δ é injetiva.

Também temos que, para toda dupla (a, b) em $\mathbb{R} \times \mathbb{R} = CD(\delta)$, $\exists$ um número complexo $a + bi$ em $\mathbb{C} = \mathrm{D}(\delta)$, tal que $\delta(a + bi) = (a, b)$. Portanto, também temos que δ é sobrejetiva.

Por fim, $\forall\ a + bi, c + di \in \mathbb{C} = D(\delta)$, temos $\delta\big((a + bi) + (c + di)\big) = \delta\big((a + c) + (b + d)i\big) = (a + c, b + d) = (a, b) + (c, d) = \delta(a + bi) + \delta(c + di)$. E, também, $\delta\big((a + bi)(c + di)\big) = \delta\big((ac + bd).(ad + bc)i\big) = (ac - bd, ad + bc) = (a, b)(c, d) = \delta(a + bi)\delta(c + di)$. Isso mostra que $\mathbb{C}$ é isomorfo a $\mathbb{R}^2$.∎

Olhando a definição de produto cartesiano em 1.1.4, entendemos que, em geral, temos $A \times B \neq B \times A$. Além disso, a equivalência $a = c$ e $b = d \Leftrightarrow (a, b) = (c, d)$, usada para mostrar a injetividade da função δ, depende do conceito de igualdade entre pares ordenados, o que consideramos entendido.

Agora, consideremos as operações usuais de adição e multiplicação de matrizes no conjunto $\mathsf{C} = \left\{ \begin{bmatrix} x & y \\ -y & x \end{bmatrix}_{2x2} / x, y \in \mathbb{R} \right\}$. Podemos definir uma função que identifica cada número $z = a + bi$ de $\mathbb{C}$ como uma matriz $A = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}_{2x2}$ de C. Esse isomorfismo, então, nos dá mais uma versão concreta de um número complexo.

Não será provado esse isomorfismo pois é realizada de forma análoga ao que foi demonstrado anteriormente, mas podemos observar a validade da propriedade a) descrita em 1.4.2.

Tomemos a seguinte função:

$$\delta: \mathbb{C} \longrightarrow \mathsf{C}$$
$$a + bi \mapsto \delta(a + bi) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}_{2x2}$$

Seja $e = 0{+}0\mathrm{i}$, o elemento neutro aditivo em $\mathbb{C}$, temos que $\varphi(e) = \varphi(0 + 0i) = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}_{2x2} = e'$, elemento neutro aditivo em C, assim $\varphi(e) = e'$.

Tomando-se $e = 1{+}0\mathrm{i}$, o elemento neutro multiplicativo em $\mathbb{C}$, temos que $\varphi(e) = \varphi(1 + 0i) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}_{2x2} = e'$, o elemento neutro multiplicativo em C e do mesmo modo $\varphi(e) = e'$.

Capítulo 2 – A Álgebra dos Vértices de um Polígono Regular

Neste capítulo mostraremos que o conjunto dos vértices de um polígono regular tem a mesma estrutura algébrica que a do conjunto quociente, determinado pela congruência módulo n, de modo aditivo.

Mostraremos que é possível definir um homomorfismo bijetivo de modo a comparar o conjunto das raízes de ordem n da unidade complexa, que podem ser representadas geometricamente no plano cartesiano, com o conjunto $\mathbb{Z}_n$.

§2.1 Polígonos Regulares

2.1.1 Definição: Um polígono é chamado de *regular* se, e somente se, tem todos os seus lados e todos os seus ângulos internos congruentes.

Esse conceito já aparece nos estudos secundários quando estudamos a área das figuras planas, longe de sabermos da engenhosidade geométrica envolvida na construção desses objetos, a depender das ferramentas que podem ser usadas.

De início iremos explicar, passo a passo, como construir alguns polígonos regulares, utilizando o GEOGEBRA, que é, na atualidade, mais uma ferramenta que podemos utilizar.

2.1.2 O passo a passo da construção de um triângulo equilátero

1. Marcamos um ponto A e um ponto B;

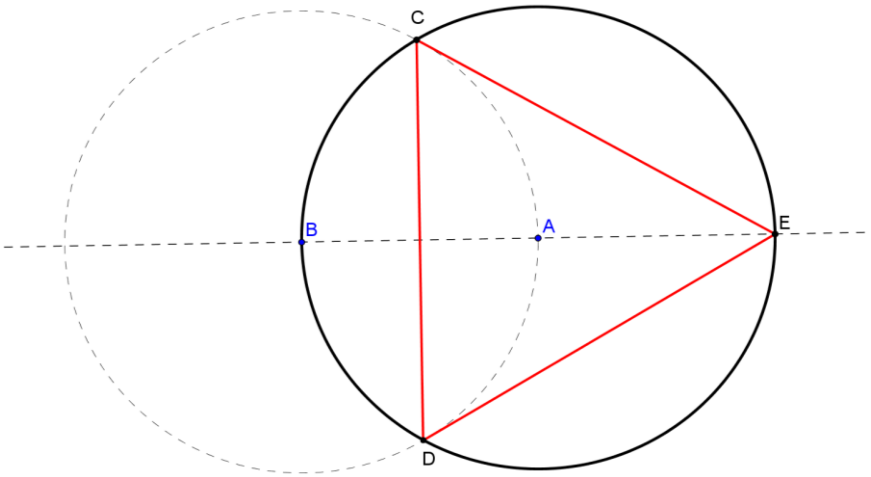
2. Traçamos uma circunferência λ_1, centrada em A e que passe em B, e uma circunferência λ_2, de centro em B e que passe em A;

3. Marcamos os pontos C e D, de intersecção entre essas duas circunferências;

4. Traçamos a reta $\overleftrightarrow{AB}$ e marcamos o ponto E na circunferência λ_1;

5. Ligando os pontos C, D e E, obtemos o triângulo CDE que é um triângulo equilátero inscrito na circunferência λ_1, de centro em A e raio r $=\overline{AB}$.

Figura 03: Construção de um triângulo equilátero



2.1.3 O passo a passo da construção de um quadrado

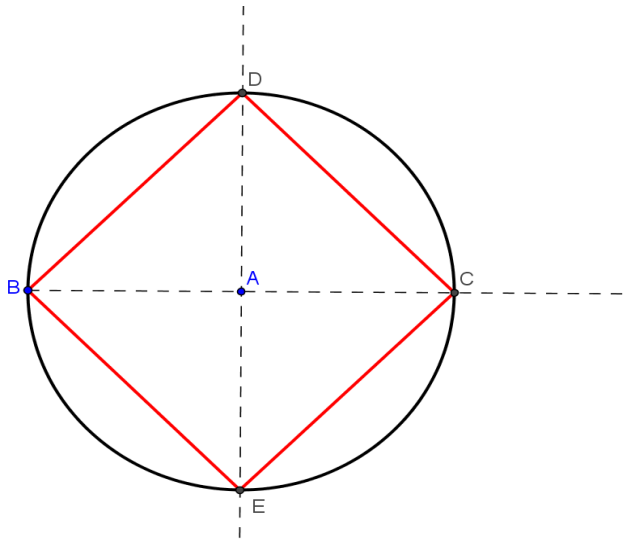
1. Marcamos um ponto A e um ponto B e constrói-se a circunferência λ, de centro em A e que passa por B;

2. Traçamos a semi reta $\overrightarrow{BA}$, determinando C, o ponto de interseção dessa semi reta com a circunferência;

3. Traçamos a mediatriz do segmento $\overline{BC}$, determinando os pontos D e E, de interseção dessa mediatriz com a circunferência;

4. Ligando os pontos B, C, D e E, obtemos o quadrado BCDE inscrito na circunferência λ.

Figura 04: Construção de um quadrado



2.1.4 O passo a passo da construção de um pentágono

1. Marcamos um ponto A e um ponto B e construímos a circunferência λ, de centro em A e que passa por B;

2. Traçamos a perpendicular ao segmento $\overline{AB}$ que passa em A, determinando o ponto C sobre λ;

3. Marcamos D, o ponto médio de AC;

4. Traçar a bissetriz de $A\hat{D}B$ e encontramos o ponto H sobre o segmento $\overline{AB}$;

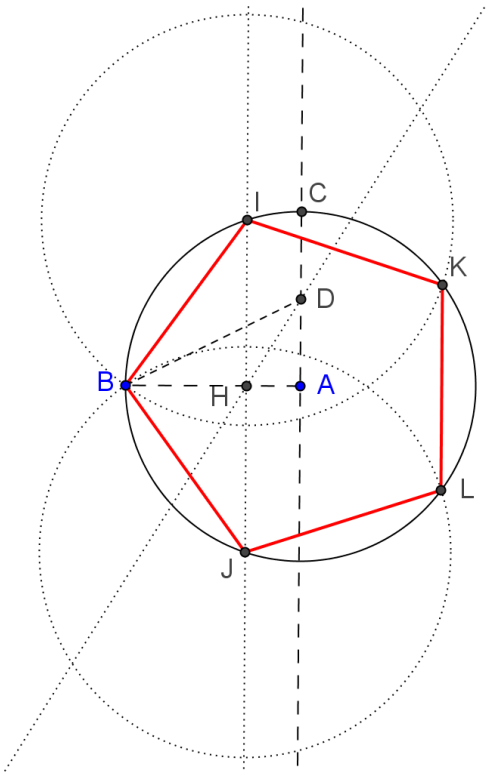
5. Traçamos uma perpendicular a $\overline{AB}$ no ponto H, encontrando os pontos I e J, interseção dessa perpendicular com λ;

6. Traçamos uma circunferência de centro em I e que passa pelo ponto B, encontrando o ponto K, outra intersecção dessa circunferência com λ;

7. Traçamos uma circunferência de centro em J e que passa pelo ponto B, encontrando o ponto L, outra intersecção dessa circunferência com λ;

8. Ligando os pontos BIKLJ, obtemos o pentágono regular inscrito na circunferência λ.

Figura 05: Construção de um pentágono regular



2.1.5 O passo a passo da construção de um hexágono regular

1. Marcamos um ponto A e um ponto B;

2. Traçamos uma circunferência λ_1, centrada em A e que passe em B e uma circunferência λ_2, de centro em B e que passe em A;

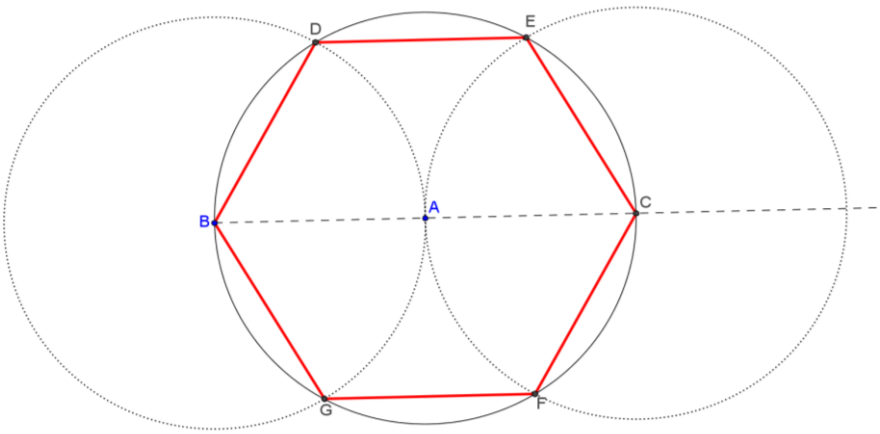
3. Traçamos a semi reta $\overrightarrow{BA}$, determinando o ponto C, intersecção dessa semi reta com a circunferência λ_1;

4. Traçamos a circunferência λ_3, de centro em C e que passa por A;

5. As intersecções de λ_2 e λ_3 com λ_1, chamamos de D, E, F e G;

6. Ligando os pontos BDECFG, obtemos o hexágono regular inscrito na circunferência λ_1.

Figura 06: Construção de um hexágono regular



A construção que faremos a seguir, tendo por base as medidas obtidas no processo descrito anteriormente, é uma aproximação satisfatória do heptágono regular. Em 1726, Gauss, aos 19 anos, mostrou que a construção do heptágono regular e de outros polígonos regulares era impossível através de processos euclidianos, investigou ainda a construtibilidade dos polígonos regulares de p lados, sendo p um número primo.

Nessa investigação Gauss provou o seguinte resultado:

2.1.6 Observação (Teorema de Gauss-Wantzel): Um polígono regular de n lados pode ser construído com régua e compasso se, e somente se, $n = 2^{\alpha}$ ou $n = 2^{\alpha}p_1p_2 \cdots p_r$; onde p_1, p_2, ... , p_r são números primos distintos da forma $p = 2^{2^{\beta}} + 1$ e α e β são números inteiros; ou seja, são números primos de Fermat.

Demonstração (Ver [6]; pág. 200) .■

Os três primeiros números de Fermat são $3 = 2^{2^0} + 1$, $5 = 2^{2^1} + 1$ e $17 = 2^{2^2} + 117$. Assim, usando as construções de Euclides e o resultado de Fermat, podemos afirmar que:

a) É possível construir os seguintes polígonos (até 20 lados): os de 3, 4, 5, 6, 8, 10, 12, 15, 16, 17 e 20 lados, incluindo todos os construídos por Euclides, tendo em vista que podemos escrever: $3 = 2^0.3$, $4 = 2^2$, $5 = 2^0.5$, $6 = 2^1.3$, $8 = 2^3$; $10 = 2^1.5$, $12 = 2^2.3$, $15 = 2^0.3.5$, $16 = 2^4$, $17 = 2^0.17$ e $20 = 2^2.5$.

b) Os polígonos regulares de 7, 9 e 27 lados não são construtíveis com o uso de régua e compasso.

c) Os polígonos regulares com um número primo de lados são, portanto, o triângulo e o pentágono, construídos por Euclides e os de lados $n = 2^{2^{\beta}} + 1$.

Como se sabe, $n = 2^{2^{\beta}} + 1$ é primo para $\beta = 0, 1, \cdots, 4$; ou seja, $n = 3, 5, 17, 257$ ou 65.537. Euler mostrou que para $\beta = 5$, $n = 2^{2^5} + 1 = 641 \times 6.700.417$ é composto. Até o momento não foi encontrado outro número primo dessa forma.

2.1.7 O passo a passo da construção (aproximada) de um heptágono regular

1. Marcamos os pontos A e B e traçamos a semi reta $\overrightarrow{AB}$;

2. Traçamos a circunferência λ_1, de centro em B, passando por A e determinando o ponto M na semi reta $\overrightarrow{AB}$;

3. Traçamos uma perpendicular à semi reta $\overrightarrow{AB}$, no ponto B;

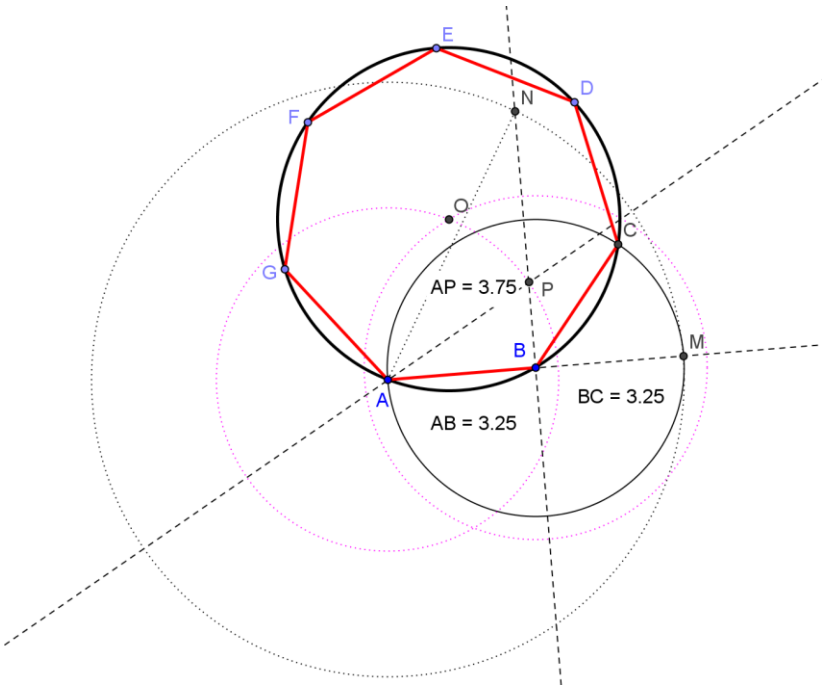
4. Traçamos a circunferência λ_2, de centro em A, passando por M e determinando sobre essa perpendicular o ponto N;

5. Traçamos a bissetriz do ângulo $M\hat{A}N$, determinando o ponto P sobre $\overline{BN}$;

6. Traçamos duas circunferências. Uma com centro em A que passa por P e outra com centro em B de mesmo raio que a anterior. Na interseção dessas duas circunferências marcamos o ponto O. Com centro nesse ponto traçamos a circunferência que irá circunscrever o heptágono. Essa circunferência intercepta a primeira circunferência no ponto C.

7. Os segmentos $\overline{AB}$ e $\overline{BC}$ são congruentes e fazem parte dos lados do heptágono regular. Com essa medida marcamos os pontos D, E, F e G, circunferência λ_2, e traçamos o heptágono regular ABCDEFG.

Figura 07: Construção de um heptágono regular



2.1.8 O passo a passo da construção de um octógono regular

1. Marcamos um ponto A e um ponto B. Traçamos o segmento $\overline{AB}$ e marcamos o seu ponto médio O;

2. Traçamos uma circunferência λ_1, centrada em A e que passe em B e uma circunferência λ_2, de centro em B e que passe em A;

3. Traçamos a circunferência λ_3, de diâmetro $\overline{AB}$ e centro em O;

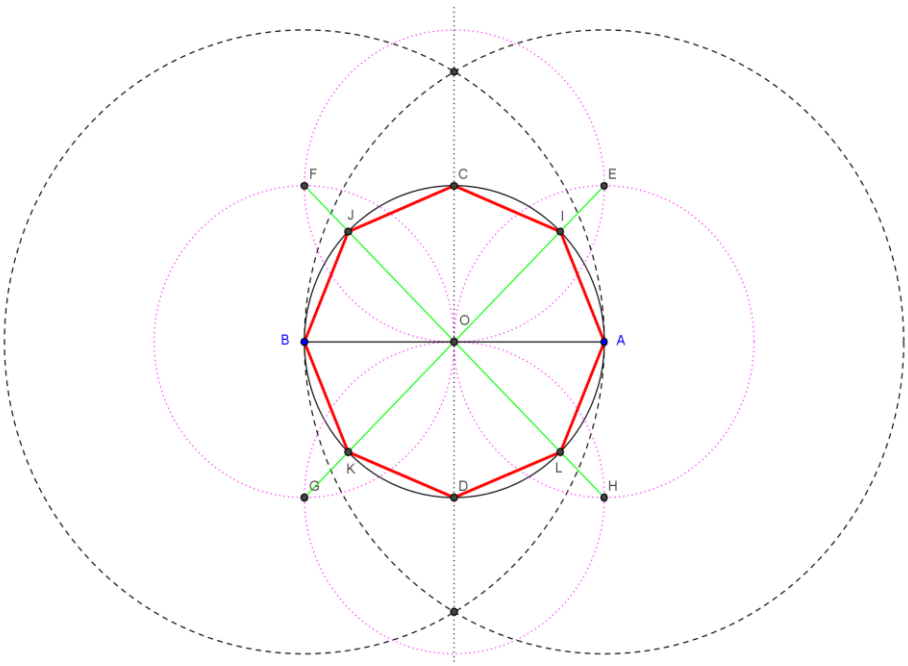
4. Traçamos a mediatriz de $\overline{AB}$ que passará pelos pontos de interseção de λ_1 e λ_2 e que interceptará a circunferência λ_3 em C e D;

5. Traçamos uma circunferência centrada em A, uma circunferência centrada em B, uma circunferência centrada em C e uma circunferência centrada em D, todas passando pelo ponto O;

6. Marcamos E, F, G e H, pontos de interseção entre essas circunferências, e traçamos os segmentos $\overline{EG}$ e $\overline{FH}$ que intersectam λ_3, nos pontos I, J, K e L;

7. O polígono BKDLAICJ é um octógono regular inscrito na circunferência λ_3;

Figura 08: Construção do octógono regular



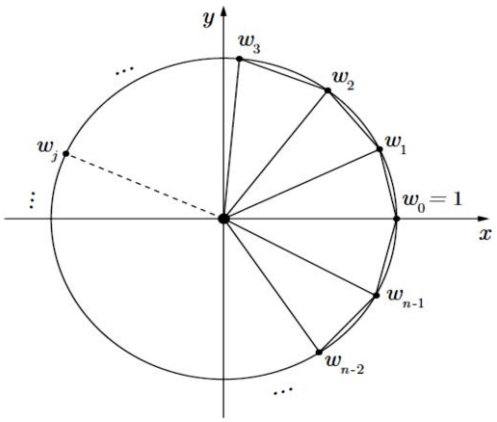
Agora mostraremos que ao representarmos geometricamente as raízes de ordem *n* da unidade complexa, acabamos por obter o desenho de um polígono regular, inscrito em um círculo unitário. Isso, de certa forma, resolve o problema da impossibilidade da construtibilidade através de régua e compasso de alguns polígonos regulares, devido a observação de Gauss em 2.1.6.

De acordo com as definições em 1.3.12, considerando a forma polar e a representação geométrica de cada raiz da unidade, podemos relacionar o seguinte resultado.

2.1.9 Observação: as n raízes de $1 = 1 + 0i \in \mathbb{C}$, $w_k = cos\frac{2k\pi}{n} + isen\ \frac{2k\pi}{n}$; com $k = 0, 1, \cdots, n-1$, ocupam os vértices de um polígono regular de n lados inscrito no círculo unitário e centrado na origem do plano de Argand – Gauss.

Demonstração: Sendo $z = 1 = 1 + 0i$, vale que $|z| = \sqrt{1^2 + 0^2} = 1$. Assim, temos $|w_k| = \sqrt{|z|} = 1$, ou seja, cada raiz está sobre uma circunferência de raio unitário e centro na origem. Além disso, observamos que $\arg(w_{k+1}) - \arg(w_k) = \frac{2\pi}{n}$, o que mostra que essas raízes ocupam os vértices de um polígono regular de n lados, inscrito no círculo unitário de centro na origem.■

Figura 09: Representação geométrica das raízes enésimas da unidade



2.1.10 Uma representação geométrica das raízes de ordem 2 da unidade

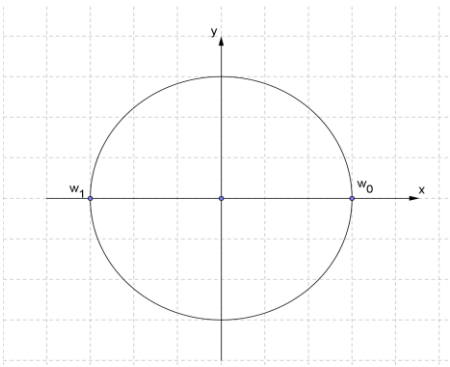
De acordo com nossa observação em 1.3.14, temos que as raízes quadradas da unidade são:

$w_0 = cos0 + isen\ 0 = 1 + 0i$;

$w_1 = cos\pi + isen\pi = -1 + 0i$.

Isso nos dá a representação geométrica abaixo

Figura 10: Representação geométrica das raízes quadradas da unidade



2.1.11 Uma representação geométrica das raízes de ordem 3 da unidade

As raízes cúbicas da unidade são:

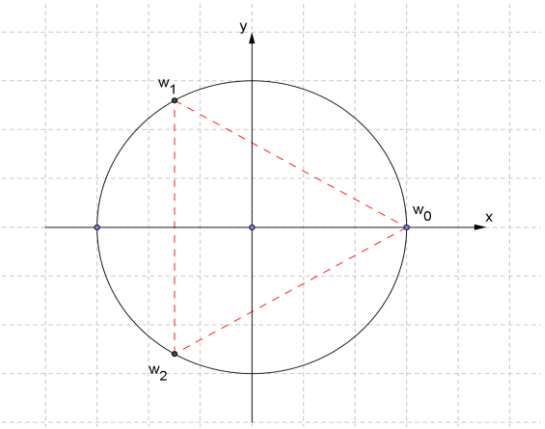
$w_0 = cos0 + isen\ 0 = 1 + 0i;$

$w_1 = cos\frac{2\pi}{3} + isen\frac{2\pi}{3} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i;$

$w_2 = cos\frac{4\pi}{3} + isen\frac{4\pi}{3} = -\frac{1}{2} - \frac{\sqrt{3}}{2}i.$

Isso nos dá a representação geométrica abaixo

Figura 11: Representação geométrica das raízes cúbicas da unidade



2.1.12 Uma representação geométrica das raízes de ordem 4 da unidade

As raízes são:

$w_0 = cos0 + isen\ 0 = 1 + 0i;$

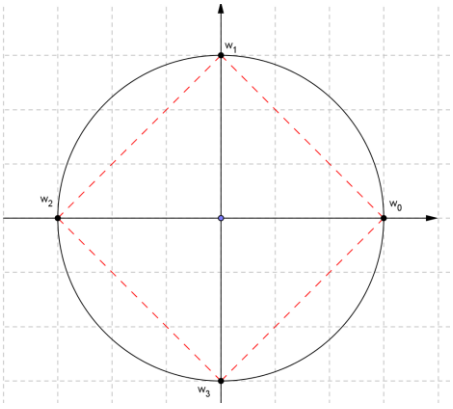
$w_1 = cos\frac{\pi}{2} + isen\frac{\pi}{2} = 0 + 1i;$

$w_2 = cos\pi + isen\pi = -1 + 0i;$

$w_3 = cos\frac{3\pi}{2} + isen\frac{3\pi}{2} = 0 + (-1)i.$

Isso nos dá a representação geométrica abaixo

Figura 12: Representação geométrica das raízes quartas da unidade



2.1.13 Uma representação geométrica das raízes de ordem 5 da unidade

As raízes são:

$w_0 = cos0 + isen\ 0$

$w_1 = cos\frac{2\pi}{5} + isen\frac{2\pi}{5};$

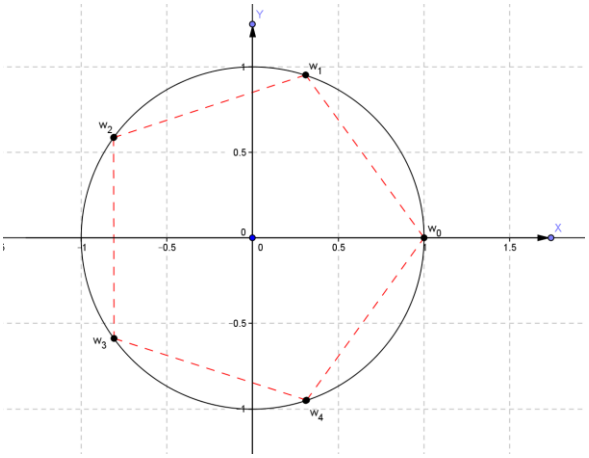
$w_2 = cos\frac{4\pi}{5} + isen\frac{4\pi}{5};$

$w_3 = cos\frac{6\pi}{5} + isen\frac{6\pi}{5};$

$w_4 = cos\frac{8\pi}{5} + isen\frac{8\pi}{5};$

Isso nos dá a representação geométrica abaixo

Figura 13: Representação geométrica das raízes quintas da unidade



Sabemos, devido a Gauss, como mencionamos na observação 2.1.6, que não podemos construir, com régua e compasso, um polígono regular de 7 lados. Mas, fazendo a representação geométrica das raízes de ordem 7 da unidade complexa, podemos, facilmente, construir o heptágono de forma bem precisa, através do GEOGEBRA.

2.1.14 Uma representação geométrica das raízes de ordem 7 da unidade

As raízes são:

$w_0 = cos0 + isen\ 0 = 1 + 0i;$

$w_1 = cos\frac{2\pi}{7} + isen\frac{2\pi}{7};$

$w_2 = cos\frac{4\pi}{7} + isen\frac{4\pi}{7};$

$w_3 = cos\frac{6\pi}{7} + isen\frac{6\pi}{7}$;

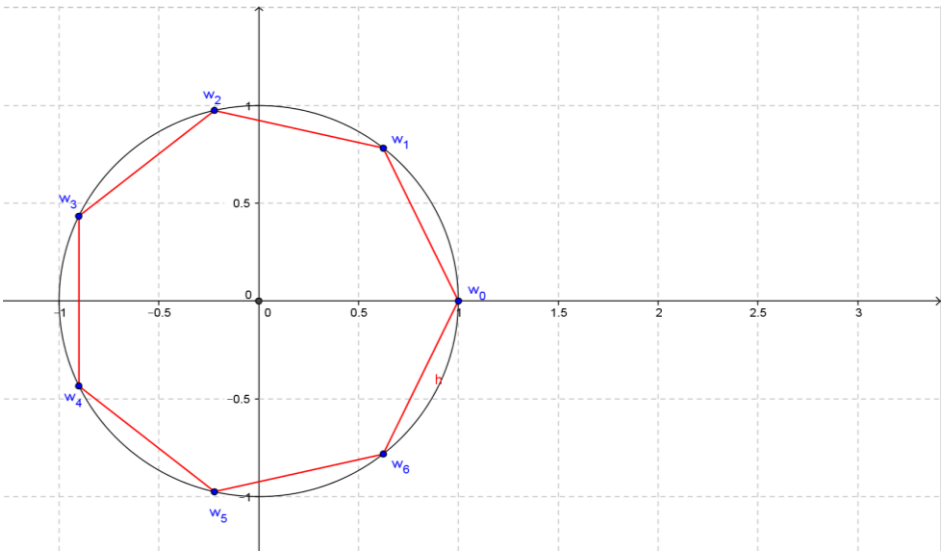
$w_4 = cos\frac{8\pi}{7} + isen\frac{8\pi}{7}$;

$w_5 = cos\frac{10\pi}{7} + isen\frac{10\pi}{7}$;

$w_6 = cos\frac{12\pi}{7} + isen\frac{12\pi}{7}$;

Isso nos dá a representação geométrica abaixo

Figura 14: Representação geométrica das raízes sétimas da unidade



Da mesma forma, conseguimos construir os polígonos de 9 e 27 lados com mais precisão.

De maneira geral, destacamos a facilidade que é, através da representação geométrica das raízes da unidade complexa, construir um polígono regular de $2 < n$ lados.

Seguimos fazendo, ainda, o uso de construções geométricas como parte da discussão em torno do principal objetivo de nosso trabalho, que é o de podermos mostrar que a estrutura do conjunto desses pontos do plano, que determinam um polígono regular de $2 < n$ lados, pode ser comparada, aditivamente, à estrutura do conjunto das classes determinada pela relação congruência módulo n, inteiro.

Doravante, $\mathbb{U}_n = \left\{w_k = cos\frac{2k\pi}{n} + isen\frac{2k\pi}{n} / 2 < n \in \mathbb{Z} \text{ e } k = 0, 1, \cdots, n-1\right\}$ denotará *o conjunto das raízes de ordem* $2 < n$ *da unidade complexa*.

§ 2.2 A multiplicação de números complexos no conjunto $\mathbb{U}_n$

Conhecemos do Cálculo Diferencial que, usando séries de potências, podemos escrever a identidade de Euler: $e^{i\theta} = cos\theta + isen\theta$.

Através dessa relação podemos observar qual o efeito ao multiplicarmos duas raízes da unidade complexa. Em geral, escrevendo um número complexo na forma $z = |z|(\cos\theta + i\text{sen}\theta) = |z|e^{i\theta}$, teríamos, para cada $k = 0, 1, \cdots, n-1$, as raízes de ordem n da forma $w_k = e^{\frac{2k\pi i}{n}}$. E, perceberíamos o efeito somativo no expoente desse produto.

Mas, apostamos no entendimento de que podemos fazer uma boa comparação desses objetos e, mesmo evitando o uso dos conceitos do cálculo diferencial, entender como objetos da Geometria (de Euclides) surgem como elementos de uma Estrutura Algébrica e, vice versa.

2.2.1 Exemplos de conjuntos que não suportam a multiplicação definida em $\mathbb{C}$:

Exemplo 1: $A = \{z \in \mathbb{C} / z^4 = 2\}$

Através de contas simples, vemos que

$$A = \left\{\sqrt[4]{2}, \sqrt[4]{2}\left(cos\ \frac{\pi}{2} + isen\ \frac{\pi}{2}\right), \sqrt[4]{2}(cos\pi\ + isen\pi), \sqrt[4]{2}\left(cos\ \frac{3\pi}{2} + isen\ \frac{3\pi}{2}\right)\right\}$$

Calculando, por exemplo, algumas potências de $w_1 = \sqrt[4]{2}\left(cos\ \frac{\pi}{2} + isen\ \frac{\pi}{2}\right)$, temos:

$$w_1 = \sqrt[4]{2}\left(cos\ \frac{\pi}{2} + isen\ \frac{\pi}{2}\right),$$

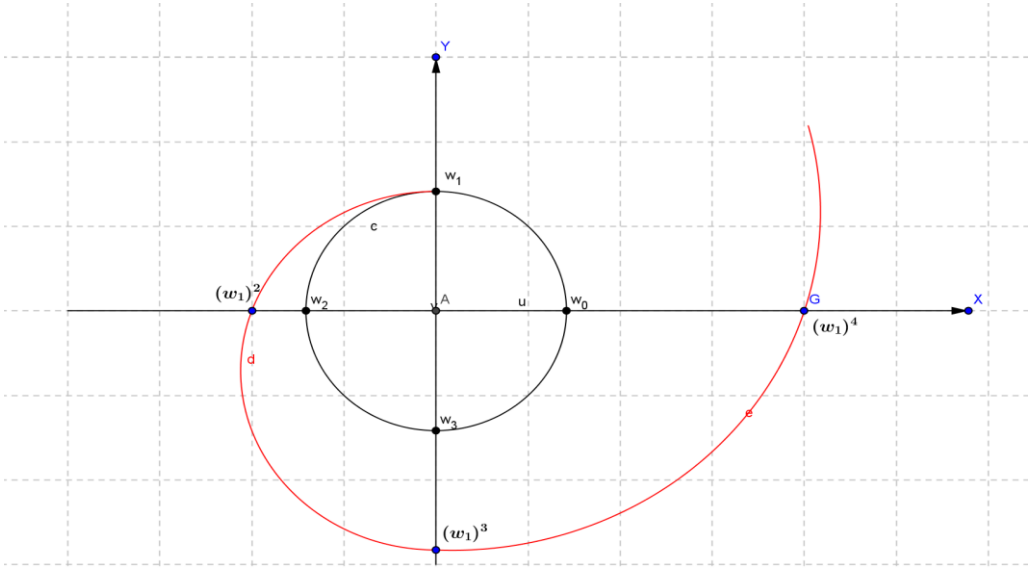
$$w_1^2 = w_1 w_1 = \left(\sqrt[4]{2}\right)^2\left(cos\ \left(\frac{\pi}{2} + \frac{\pi}{2}\right) + isen\left(\frac{\pi}{2} + \frac{\pi}{2}\right)\right) = \sqrt{2}(cos\pi\ + isen\,\pi),$$

$$w_1^3 = w_1^2 w_1 = \sqrt{2}(cos\pi\ + isen\,\pi)\sqrt[4]{2}\left(cos\ \frac{\pi}{2} + isen\ \frac{\pi}{2}\right) = \sqrt[4]{2^3}\left(cos\ \frac{3\pi}{2} + isen\ \frac{3\pi}{2}\right)$$

$$w_1^4 = w_1^3 w_1 = \sqrt[4]{2^3}\left(cos\ \frac{3\pi}{2} + isen\ \frac{3\pi}{2}\right)\sqrt[4]{2}\left(cos\ \frac{\pi}{2} + isen\ \frac{\pi}{2}\right) = 2(cos2\pi + isen2\pi)$$

Podemos observar, na figura 15 abaixo que, embora as raízes quartas de $z = 2$ possam representar vértices de um quadrado, as potências de w_1 "explodem", no sentido de que o módulo dessas potências aumenta e as afasta do conjunto A, quando as afasta da origem do plano. Isso, claro, também mostra que A não é fechado para a multiplicação definida em $\mathbb{C}$.

Figura 15: Representação das raízes quartas de $z = 2$ e potências de $w_1 = \sqrt[4]{2}\left(cos\ \frac{\pi}{2} + isen\ \frac{\pi}{2}\right)$



Exemplo 2: $B = \left\{z \in \mathbb{C}/z^4 = \frac{1}{2}\right\}$

Através de contas simples, vemos que

$$B = \left\{\sqrt[4]{\frac{1}{2}}, \sqrt[4]{\frac{1}{2}}\left(cos\ \frac{\pi}{2} + isen\ \frac{\pi}{2}\right), \sqrt[4]{\frac{1}{2}}(cos\pi\ + isen\pi), \sqrt[4]{\frac{1}{2}}\left(cos\ \frac{3\pi}{2} + isen\ \frac{3\pi}{2}\right)\right\}$$

Calculando, por exemplo, algumas potências de $w_1 = \sqrt[4]{\frac{1}{2}}\left(cos\ \frac{\pi}{2} + isen\ \frac{\pi}{2}\right)$, temos:

$$w_1 = \sqrt[4]{\frac{1}{2}}\left(cos\ \frac{\pi}{2} + isen\ \frac{\pi}{2}\right),$$

$$w_1^2 = w_1 w_1 = \left(\sqrt[4]{\frac{1}{2}}\right)^2\left(cos\ \left(\frac{\pi}{2} + \frac{\pi}{2}\right) + isen\left(\frac{\pi}{2} + \frac{\pi}{2}\right)\right) = \sqrt{\frac{1}{2}}(cos\pi\ + isen\,\pi),$$

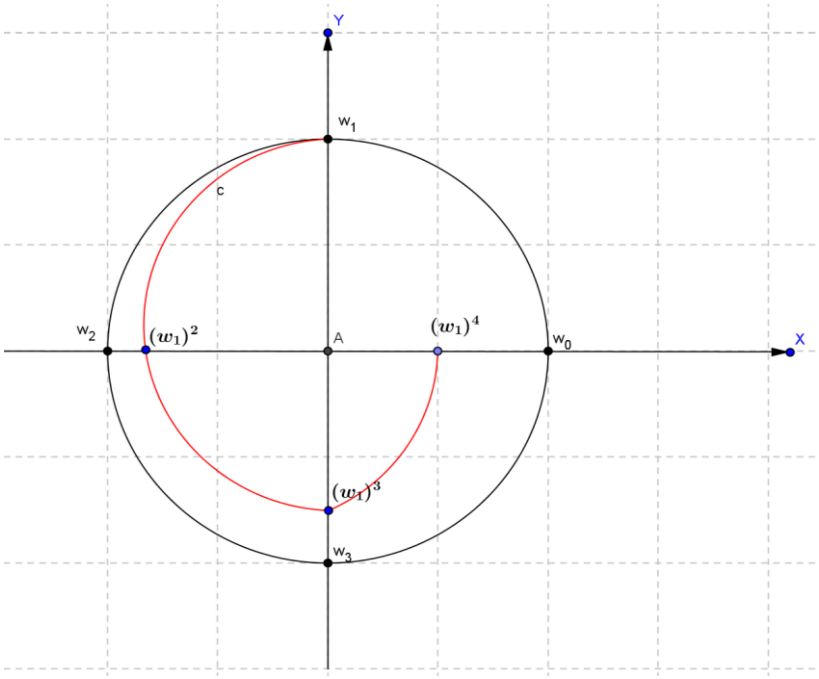
$$w_1^3 = w_1^2 w_1 = \sqrt{\frac{1}{2}}(cos\pi\ + isen\,\pi)\sqrt[4]{\frac{1}{2}}\left(cos\ \frac{\pi}{2} + isen\ \frac{\pi}{2}\right) = \sqrt[4]{\frac{1}{2^3}}\left(cos\ \frac{3\pi}{2} + isen\ \frac{3\pi}{2}\right)$$

$$w_1^4 = w_1^3 w_1 = \sqrt[4]{\frac{1}{2^3}}\left(cos\ \frac{3\pi}{2} + isen\ \frac{3\pi}{2}\right)\sqrt[4]{\frac{1}{2}}\left(cos\ \frac{\pi}{2} + isen\ \frac{\pi}{2}\right) = \frac{1}{2}(cos2\pi + isen2\pi)$$

Mais uma vez vemos que, embora as raízes quartas de $z = \frac{1}{2}$ possam representar vértices de um quadrado, as potências de w_1 "encolhem", no sentido de que o módulo dessas potências diminui e as afasta do conjunto A, enquanto as

aproxima da origem do plano. Por isso, também concluímos que B não é fechado para a multiplicação definida em $\mathbb{C}$.

Figura 16: Representação das raízes quartas de $z = \frac{1}{2}$ e potências de $w_1 = \sqrt[4]{\frac{1}{2}}\left(cos\ \frac{\pi}{2} + isen\ \frac{\pi}{2}\right)$



Em nosso próximo exemplo, para não induzir um pensamento errado, consideraremos que z não seja um número "real puro", onde $\mathrm{Im}(z) = 0$.

Mesmo assim, o exemplo trata de um caso muito particular de cálculo de raízes e potências de um número complexo.

Exemplo 3: $C = \left\{z \in \mathbb{C}/z^4 = \frac{1}{2} + \frac{\sqrt{3}}{2}i\right\}$

Note que $|z| = \sqrt{\left(\frac{1}{2}\right)^2 + \left(\frac{\sqrt{3}}{2}\right)^2} = 1$ e, através de contas simples, vemos que

$$C = \left\{cos\frac{\pi}{12} + isen\frac{\pi}{12}, cos\frac{7\pi}{12} + isen\frac{7\pi}{12}, cos\frac{13\pi}{12} + isen\frac{13\pi}{12}, cos\frac{19\pi}{12} + isen\frac{19\pi}{12}\right\}$$

Calculando algumas potências de $w_1 = cos\frac{7\pi}{12} + isen\frac{7\pi}{12}$, temos:

$$w_1 = cos\frac{7\pi}{12} + isen\frac{7\pi}{12},$$

$$w_1^2 = w_1 w_1 = cos\left(\frac{7\pi}{12} + \frac{7\pi}{12}\right) + isen\left(\frac{7\pi}{12} + \frac{7\pi}{12}\right) = cos\frac{7\pi}{6} + isen\frac{7\pi}{6},$$

$$w_1^3 = w_1^2 w_1 = \left(cos\frac{7\pi}{6} + isen\frac{7\pi}{6}\right)\left(cos\frac{7\pi}{12} + isen\frac{7\pi}{12}\right) = cos\ \frac{7\pi}{4} + isen\ \frac{7\pi}{4}$$

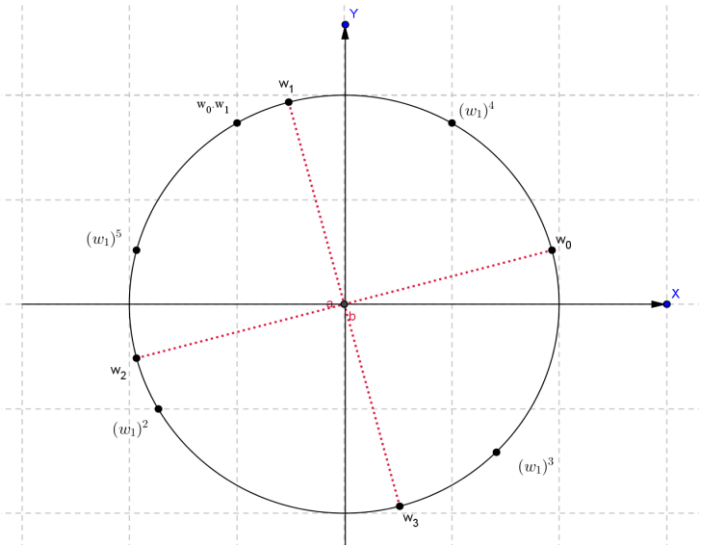
$$w_1^4 = w_1^3 w_1 = \left(cos\frac{7\pi}{4} + isen\frac{7\pi}{4}\right)\left(cos\frac{7\pi}{12} + isen\frac{7\pi}{12}\right) = cos\ \frac{7\pi}{3} + isen\ \frac{7\pi}{3}$$

$$w_1^5 = w_1^4 w_1 = \left(cos\frac{7\pi}{3} + isen\frac{7\pi}{3}\right)\left(cos\frac{7\pi}{12} + isen\frac{7\pi}{12}\right) = cos\ \frac{35\pi}{12} + isen\ \frac{35\pi}{12}$$

Percebemos, na figura 17 logo abaixo, que o argumento de w_1^n, com $n = 1, 2, 3, 4$ ou 5; não coincide com nenhum dos argumentos das raízes quartas de $z = \frac{1}{2} + \frac{\sqrt{3}}{2}i$ e assim, a representação geométrica dessas potências não pode coincidir com a representação geométrica dessas raízes.

Além disso, notemos que $w_0 w_1 = cos\frac{8\pi}{12} + isen\frac{8\pi}{12} \neq w_k,\ \forall\ k \in \{0,1,2,3\}$, mostrando que C não é multiplicativamente fechado.

Figura 17: Representação das raízes quartas de $z = \frac{1}{2} + \frac{\sqrt{3}}{2}i$ e potências de $w_1 = cos\ \frac{7\pi}{12} + isen\ \frac{7\pi}{12}$



Notemos que, independentemente dos números complexos que consideramos nesses exemplos, o desenho de um polígono regular, no caso de um quadrado, sempre pode ser feito. O que poderia tornar sem sentido querer comparar o conjunto dos vértices de polígonos regulares, considerando somente o conjunto $\mathbb{U}_n$ das raízes da unidade complexa. Mas, o problema com o fechamento da multiplicação visto nesses exemplos, justifica nossa ideia de olhar exatamente no conjunto desses objetos geométricos. Esse é um dos cuidados que temos que ter e que dá sentido aos nossos esforços para tentar comparar $\mathbb{U}_n$ com outro arcabouço onde, de certo, já sabemos que podemos manipular objetos com segurança.

2.2.3 Observação: O Conjunto $\mathbb{U}_n$, formado pelas raízes enésimas da unidade complexa, é multiplicativamente fechado.

Demonstração: Basta lembrar as discussões e a definição de *argumento* (*principal*) *do número complexo z*, feitas na definição em 1.3.12. A unicidade do ângulo $\theta = \arg(z) \in]-\pi, \pi]$ e a regra de que o produto de dois números complexos, na forma polar, é igual a um número complexo cujo módulo é o produto dos módulos e cujo argumento é a soma dos argumentos dos números complexos multiplicados, mostram que o resultado da multiplicação de dois elementos de $\mathbb{U}_n$ é também uma raiz de ordem n da unidade complexa.∎

§ 2.3 A Álgebra dos Vértices de um Polígono Regular Inscrito no Círculo Trigonométrico.

Conforme nossa observação em 2.2.3, podemos manipular as raízes da unidade complexa com certa segurança. Isso é um convite para investigarmos as propriedades da multiplicação definida em $\mathbb{U}_n$.

Na forma polar, cada raiz da unidade complexa tem módulo igual a 1 e, por isso, de acordo com nossas discussões em 1.3.12, multiplicar esses objetos significa, efetivamente, efetuar uma soma.

2.3.1 Observação: Com relação à multiplicação, valem as seguintes propriedades, $\forall$ $w_h, w_j, w_l \in \mathbb{U}_n = \left\{w_k = cos\frac{2k\pi}{n} + isen\frac{2k\pi}{n} / \, 2 < n \in \mathbb{Z} \text{ e } k = 0, 1, \cdots, n-1\right\}$:

$-$ Associatividade: $w_h\,(w_j w_l) \;= \left(w_h w_j\right) w_l$;

$-$ Comutatividade: $w_h w_j = w_j w_h$;

$-$ Existência de elemento neutro: $\exists\, 1 + 0i = w_0 = cos\frac{2.0.\pi}{n} + isen\frac{2.0.\pi}{n} = cos0 + isen0$, tal que $(1 + 0i)w_h = w_h(1 + 0i) = w_h$;

$-$ Existência de inverso: $\forall w_h \in \mathbb{U}_n, \exists\, w_g \in \mathbb{U}_n$, tal que, sendo $w_g = cos\frac{2g\pi}{n} + isen\frac{2g\pi}{n}$, vale que $w_h w_g = w_g w_h = 1 = 1 + 0i$.

Demonstração: As propriedades de associatividade e comutatividade valem, por herança, de $\mathbb{C}$ para $\mathbb{U}_n$. Como $1 = w_0 = cos\frac{2.0.\pi}{n} + isen\frac{2.0.\pi}{n} = cos0 + isen0$ é uma raiz da unidade, a existência de elemento neutro está garantida.

Agora, sendo $w_h = cos\frac{2h\pi}{n} + isen\frac{2h\pi}{n}$, com $h = 0, 1, \cdots, n-1$, basta tomar $g = n - h$ para termos $w_h w_g = w_g w_h = (1 + 0i) = w_0$.■

Continuaremos com os nossos argumentos de modo que, neste parágrafo final do desenvolvimento de nosso trabalho, possamos dar uma ideia de como o conjunto $\mathbb{U}_n$, vértices de um polígono regular, pode ser visto como uma estrutura algébrica.

Olhemos por um momento as tábuas das operações de adição e multiplicação em $\mathbb{Z}_3$ e em $\mathbb{U}_3$, respectivamente.

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

$.$	w_0	w_1	w_2
w_0	w_0	w_1	w_2
w_1	w_1	w_2	w_0
w_2	w_2	w_0	w_1

Quem olha, mesmo sabendo que a tabela acima e do lado direito provém de uma multiplicação, tende a acompanhar o raciocínio da soma feita na tabela da esquerda, olhando os índices do rodapé de w_k com $k = 0, 1, 2$.

Nesse sentido, o resultado abaixo nos mostra que podemos comparar $\mathbb{U}_n$ com o conjunto das classes de equivalência $\mathbb{Z}_n$.

2.3.2 Observação: A função δ definida abaixo é um homomorfismo bijetor.

$$\begin{array}{rcl} \delta\colon (\mathbb{U}_n, .) & \longrightarrow & (\mathbb{Z}_n, +) \\ w_k & \longmapsto & \delta(w_k) = \bar{k} \end{array}$$

Demonstração: Primeiramente, $\forall\, w_j, w_l \in \mathbb{U}_n = \mathrm{D}(\delta)$, domínio da função δ, se temos $\delta(w_j) = \delta(w_l)$, então vale que $\bar{j} = \bar{l}$. Pela observação em 1.1.20 temos $j = l$, consequentemente, $w_j = w_l$ e δ é injetiva. Agora, para toda classe $\bar{x} \in \mathbb{Z}_n = \mathrm{CD}(\delta)$, contradomínio da função δ, vale que o inteiro $x \in \{0, 1, \cdots, n-1\}$, conforme a observação em 1.2.9. Assim, para esse x, a raiz da unidade $w_x \in \mathbb{U}_n = \mathrm{D}(\delta)$ é tal que $\delta(w_x) = \bar{x}$, o que prova a sobrejetividade da função δ.

Por fim, veremos que δ é um homomorfismo. De fato, $\forall\, w_j, w_l \in \mathbb{U}_n = \mathrm{D}(\delta)$, vale que $\delta(w_j.w_l) = \delta\left(\left(cos\,\frac{2j\pi}{n} + isen\,\frac{2j\pi}{n}\right).\left(cos\,\frac{2l\pi}{n} + isen\,\frac{2l\pi}{n}\right)\right)$. Isso por sua vez vale $\delta\left(cos\left(\frac{2j\pi}{n} + \frac{2l\pi}{n}\right) + isen\left(\frac{2j\pi}{n} + \frac{2l\pi}{n}\right)\right) = \delta\left(cos\left(\frac{2(j+l)\pi}{n}\right) + isen\left(\frac{2(j+l)\pi}{n}\right)\right)$ e por isso temos $\delta\left(w_j.w_l\right) = \delta\left(w_{j+l}\right) = \overline{j+l} = \bar{j} + \bar{l} = \delta(w_j) + \delta(w_l)$. Concluímos, então, que $\mathbb{U}_n \cong \mathbb{Z}_n$.■

Esse isomorfismo, além de identificar cada raiz de ordem n da unidade complexa com uma classe $\bar{x}$ do conjunto quociente de $\mathbb{Z}$ pela relação $\equiv (mod\ n)$, diz que resultados que valem para a estrutura multiplicativa de $\mathbb{U}_n$, valem de maneira equivalente para a estrutura aditiva de $\mathbb{Z}_n$ e vice versa.

Nós iremos então, por comparação, relacionar algumas propriedades que aditivamente a estrutura de $\mathbb{Z}_n$ possui e assim, dar uma descrição mais completa da estrutura multiplicativa de $\mathbb{U}_n$.

2.3.3 Definição: Seja G um conjunto não vazio no qual a operação $*$ esteja definida. Então, se $g \in G$, definimos:

a) $\langle g\rangle = \{g^n / \ n \in \mathbb{Z}\}$ como sendo o conjunto de todas as potências inteiras (lembrar definição em 1.1.11) de $g \in G$.

b) Se a operação $*$ admite elemento neutro e (ver definição em 1.1.6 – item c)), o menor inteiro positivo t tal que $g^t = e$, é denominado de *ordem* do elemento g.

c) Se tivermos $\langle g\rangle = \{g^n / \ n \in \mathbb{Z}\} = G$, dizemos que G é um *conjunto cíclico*. Nesse caso, g é denominado de (um) *gerador* de G.

2.3.4 Exemplos: Consideremos a adição definida em 1.3.3. Assim, temos que:

a) os elementos $\bar{1}$ e $\bar{3}$ em $\mathbb{Z}_8$ são tais que $\langle\bar{1}\rangle = \langle\bar{3}\rangle = \{\bar{3}^n / \ n \in \mathbb{Z}\} = \mathbb{Z}_8$. Assim, $\mathbb{Z}_8$ é um conjunto cíclico e $\bar{1}$ e $\bar{3}$ são geradores de $\mathbb{Z}_8$.

b) $\langle\bar{2}\rangle = \{\bar{2}^n / \ n \in \mathbb{Z}\} = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}\} \neq \mathbb{Z}_8$. Assim, $\bar{2}$ não é um gerador de $\mathbb{Z}_8$.

c) (O aspecto cíclico do conjunto dos vértices de um polígono regular) Aditivamente, $\forall\ 2 < n \in \mathbb{Z}$, temos claramente que $\langle\bar{1}\rangle = \{\bar{1}^n / \ n \in \mathbb{Z}\} = \ \mathbb{Z}_n$. Então, pela especial correspondência biunívoca em 2.3.2, vemos que $\mathbb{U}_n$ é um conjunto

cíclico gerado por $w_1 = cos\frac{2\pi}{n} + isen\frac{2\pi}{n}$; ou seja, $\langle w_1 \rangle = \mathbb{U}_n$, ou de modo mais geral $< w_k >$ e $<\bar{k}>$ são geradores de $(\mathbb{U}_n, .)$ e $(\mathbb{Z}_n, +)$, respectivamente, sempre que k e n forem primos entre si.

Esse exemplo nos mostra que em um conjunto, definida uma operação, pode existir mais de um elemento gerador, como existir elemento que não o gera.

A observação a seguir nos dá uma boa ideia de como podemos aproveitar dessa identificação de que $\mathbb{U}_n$ como sendo o conjunto $\mathbb{Z}_n$.

2.3.5 Observação: Se $2 < n \in \mathbb{Z}$ e n é ímpar, vale que $\prod_{k=0}^{n-1} w_k = 1$.

Demonstração: Lembrando as discussões em nosso parágrafo 1.4, temos que

$$\delta\left(\prod_{k=0}^{n-1} w_k\right) = \delta\left(w_{0+1+\cdots(n-1)}\right) = \overline{0+1+\cdots(n-1)}.$$ E isso é,

sob a barra, claro, uma soma de uma P. A. de razão e termo inicial iguais a 1. Assim, temos que esse produto vale $\delta\left(\prod_{k=0}^{n-1} w_k\right) = \frac{\overline{n.(n-1)}}{2}$, mas como n é impar,

$n = 2k+1, k \in \mathbb{Z}$, ou seja, $\delta\left(\prod_{k=0}^{n-1} w_k\right) = \frac{\overline{n.2k}}{2} = \overline{n.k} = \bar{0}$.

Agora, δ é um homomorfismo bijetor, particularmente, δ é injetivo. E como $\delta\left(1 = w_0 = cos\frac{2.0.\pi}{n} + isen\frac{2.0.\pi}{n} = cos0 + isen0\right) = \bar{0}$, resta que $\prod_{k=0}^{n-1} w_k = 1$. ∎

E o que é $\sum_{k=0}^{n-1} w_k = w_0 + w_1 + \cdots + w_{n-1}$, se $2 < n \in \mathbb{Z}$? Curiosamente, essa soma é nula! Podemos testar isso efetuando alguns cálculos nos casos em que n é pequeno.

2.3.6 Exemplos:

a) Para $n = 2$, temos as raízes

$w_0 = cos\frac{2.0.\pi}{2} + isen\frac{2.0.\pi}{2} = cos0 + isen0 = 1$ e

$w_1 = cos\frac{2\pi}{2} + isen\frac{2\pi}{2} = cos\pi + isen\pi = -1$. Dessa forma, vale que $w_0 + w_1 = 0$.

b) Para $n = 3$, temos as raízes

$w_0 = cos\frac{2.0.\pi}{3} + isen\frac{2.0.\pi}{3} = cos0 + isen0 = 1$;

$w_1 = cos\frac{2.1.\pi}{3} + isen\frac{2.1.\pi}{3} = cos\frac{2\pi}{3} + isen\frac{2\pi}{3} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$;

$w_2 = cos\frac{4\pi}{3} + isen\frac{4\pi}{3} = -\frac{1}{2} - \frac{\sqrt{3}}{2}i$. E, mais uma vez, temos uma soma nula, que é $w_0 + w_1 + w_2 = 0$.

c) Para $n = 4$, temos as raízes

$w_0 = cos\frac{2.0.\pi}{4} + isen\frac{2.0.\pi}{4} = cos0 + isen0 = 1$;

$w_1 = cos\frac{2.1.\pi}{4} + isen\frac{2.1.\pi}{4} = cos\frac{\pi}{2} + isen\frac{\pi}{2} = 0 + i$;

$w_2 = cos\frac{4\pi}{4} + isen\frac{4\pi}{4} = -1 + 0i$.

$w_3 = cos\frac{3\pi}{2} + isen\frac{3\pi}{2} = 0 - i$. E, mais uma vez, temos uma soma nula, que é $w_0 + w_1 + w_2 + w_3 = 0$.

É claro que a soma de duas raízes da unidade não é uma raiz da unidade. Por exemplo, no caso em que $n = 4$, temos que $w_0 + w_1 = 1 + i$ não é uma raiz da unidade. Isso significa que a adição dos números complexos não está definida no conjunto $\mathbb{U}_4$.

Assim, esse fato de que essa soma é nula, que também pode ser verificado com régua e compasso, nos casos em que n é pequeno, imaginando cada elemento de $\mathbb{U}_n$ como um vetor centrado na origem do plano, não deve ser tratado, via o isomorfismo que definimos em 2.3.2.

Agora, vamos definir uma estrutura algébrica amplamente estudada e que termina por dar a noção exata da estrutura de $\mathbb{U}_n$, vista através da identificação desse conjunto com o conjunto $\mathbb{Z}_n$.

2.3.7 Definições: Seja $*$ uma operação definida em um conjunto não vazio G.

a)Dizemos que G é um *grupo* com respeito à operação $*$ (e anotamos $(G,*)$) se, e somente se, $\forall\, g_1, g_2, g_3 \in G$, valem:

− Associatividade: $(g_1 * g_2) * g_3 = g_1 * (g_2 * g_3)$;

− Existência de elemento neutro: $\exists\ e \in G$ tal que $e * g_1 = g_1 * e = g_1$;

− Existência de inverso: $\exists {g_1}^{-1} \in G$ tal que ${g_1}^{-1} * g_1 = g_1 * {g_1}^{-1} = e$.

b) Dizemos que G é um *grupo comutativo* (abeliano) se, além dessas propriedades citadas acima, valer que:

− Comutatividade: $g_1 * g_2 = g_2 * g_1$.

Finalmente, podemos, através de toda essa análise que fizemos enunciar o seguinte resultado:

2.3.8 Observação: O conjunto dos pontos dos vértices de um polígono regular, inscrito em uma circunferência de raio 1, é um grupo abeliano finito.

Demonstração: Por 1.3.4, vale que $(\mathbb{Z}_n, +)$ é um grupo abeliano, $\forall\ 2 < n \in \mathbb{Z}$. Por 2.3.2, vale que $(\mathbb{U}_n, .) \cong (\mathbb{Z}_n, +)$.∎

Considerações Finais

A experiência adquirida com os esforços em compreender os conteúdos inerentes às disciplinas de Álgebra, Aritmética e Geometria, que compõem a grade curricular do nosso mestrado PROFMAT, permitiu que pudéssemos estabelecer, com certa tranquilidade, a conectividade entre os importantes conceitos matemáticos que relacionamos aqui.

Tentamos manter o rigor na escrita e procuramos deixar claro cada definição e cada resultado que usamos no desenvolvimento deste texto. Isso permitiu que pudéssemos elucidar algumas questões e interpretar com mais carinho alguns resultados. Portanto, as discussões empregadas na elaboração deste trabalho contribuíram para nosso crescimento pessoal e, esperamos que também possam contribuir no processo de ensino aprendizagem da Matemática básica, por ser, efetivamente, um bom exemplo de interdisciplinaridade e de motivação para o uso de recursos tecnológicos como régua, compasso e computador, visto que os desenhos ilustrativos foram feitos com auxílio do Geogebra.

Temos um momento interessante e relacionado com a Geometria de Euclides, quando percebemos que, ao representarmos geometricamente as raízes de ordem n da unidade complexa, acabamos por determinar um processo "mais seguro" de se obter o desenho de um polígono regular; já que, segundo Gauss, por meio de régua e compasso, certos polígonos regulares não podem ser construídos. Com o uso do Geogebra, podemos inserir as raízes enésimas da unidade e dessa forma obter um polígono regular, independentemente do inteiro $n > 2$ adotado.

A volta que demos até conseguirmos identificar o grupo abeliano formado pelos vértices de um polígono regular, através da estrutura aditiva de $\mathbb{Z}_n$, sempre que $2< n \in \mathbb{Z}$, representa um passeio agradável pelos conceitos básicos de Álgebra e Geometria. É claro que é possível provarmos que, multiplicativamente, $U = \{z \in \mathbb{C} / |z| = 1\}$ é uma subestrutura de $\mathbb{C}$, mas isso não deixa que percebamos a conectividade que existe entre os importantes conceitos algébricos e geométricos que foram relacionados aqui.

Referências Bibliográficas:

[1] Stewart, Ian. *17 equações que mudaram o mundo*. Traduzido por George Schlesinger; 1ª edição; ZAHAR, 2013.

[2] CONTEÚDO aberto. In: Wikipédia: a enciclopédia livre. Disponível em: <https://pt.wikipedia.org/wiki/Ren%C3%A9_Descartes>. (Acesso em 23.04.2015)

[3] LAUTERT, S. L; SPINILLO, A. G. *As relações entre o desempenho em problemas de divisão e as concepções de criança sobre a divisão*. Psicologia: Teoria e Pesquisa, Brasília, v. 18, n. 3, p. 237-246, 2002.

[4] GONÇALVES, Adilson. *Introdução à álgebra*. 5ª ed. Rio de Janeiro: IMPA 2008.

[5] HEFEZ, Abramo. *Aritmética*. SBM, 2013 (Coleção PROFMAT).

[6] GONZÁLEZ, N. R; LÓPEZ, P.L; NÓVOA, E. V. *Teoría de Galois*. Santiago de Compostela. 2013. Disponível em < http://www.usc.es/regaca/Galois.pdf>. Acesso em (20.03.2015).

[7] PRECIOSO, J. Conceição; PEDROSO, Hermes Antônio. *O problema da construção de polígonos regulares de Euclides a Gauss*. Disponível em <http://www.portal.famat.ufu.br/sites/famat.ufu.br/files/Anexos/Bookpage/famat_revista_13_artigo_6_0.pdf>. (Acesso em 14.12.2014).

[8] WEISS, William A. R. (2008); An introduction to set theory. Disponível em <http://www.math.toronto.edu/weiss/set_theory.html>. (Acesso em 17.08.2014).

[9] CONTEÚDO aberto. In: Wikipédia: a enciclopédia livre. Disponível em: <https://pt.wikipedia.org/wiki/N%C3%BAmero_complexo>. (Acesso em 23.04.2015).

[10] GEOGEBRA. Software de Geometria Dinâmica. Disponível Versão 4.4.(2013). Acessado: 15 de Dez de 2014