I Workshop de Álgebra da UFG – CAC
Anel dos Inteiros Gaussianos

Vinícius Loti de Lima - *vini.loti@gmail.com*
Oliviana Xavier do Nascimento - olivianas2@hotmail.com
Danilo Sanção da Silveira (Orientador) - *sancaodanilo@gmail.com*

Resumo

Um inteiro gaussiano é um elemento da forma a+bi, onde a,b ∈ ℤ e i² = -1.

Neste texto, vamos mostrar que o conjunto dos inteiros gaussianos (ℤ[i]) é um subanel de ℂ. Além disso, mostramos que ℤ[i] não é um corpo e também que não possui divisores de zero.

Introdução

Carl Frederich Gauss, nasceu em Brunswich, na Alemanha, em 30 de abril de 1777 e foi criado em uma família muito pobre. Já antes de seus 25 anos, era famoso por seu trabalho em matemática e astronomia, aos 30 anos e durante sua vida teve uma ótima atividade científica. Foi investigando questões relacionadas à reciprocidade cúbica e à reciprocidade biquadrática, que Gauss percebeu que era mais simples trabalhar sobre ℤ[i], o anel dos inteiros de gaussianos, à que em ℤ, o conjunto dos números inteiros. Escrevemos este texto, com o objetivo de que qualquer pessoa com interesse em matemática, mas sem muitos conhecimento específicos, tivesse condições técnicas de entender.

Preliminares

Definição: Seja A um conjunto com pelo menos dois elementos munido de duas operações chamadas de adição (+) e multiplicação (•). A tripla (A, +, •) é chamada de *anel* se as seguintes propriedades forem satisfeitas:

A1) (a + b) + c = a + (b + c) , ∀ a, b, c ∈ A. *(Associatividade da adição)*

A2) a + b = b + a , ∀ a, b ∈ A. *(Comutatividade da adição)*

A3) ∃ 0 ∈ A tal que 0 + a = a , ∀ a ∈ A. *(Existência do elemento neutro da adição.)*

A4) Para todo a ∈ A, ∃ -a ∈ A tal que a + (-a) = a – a = 0. *(Existência do simétrico de todo elemento de A.)*

M1) (a • b) • c = a • (b • c) , ∀ a, b, c ∈ A. *(Associatividade da multiplicação.)*

M2) ∃ 1 ∈ A tal que 1 • a = a , ∀ a ∈ A. *(Existência da unidade.)*

AM) a • (b + c) = a • b + a • c , ∀ a, b, c ∈ A. *(Distributividade da multiplicação em relação a soma.)*

Obs.: A partir de agora, vamos denotar a multiplicação de dois elementos a • b simplesmente por ab.

Exemplos: O conjunto ℂ = { a + bi | a, b ∈ ℝ e i² = -1 } é um exemplo de anél. As operações neste conjunto são definidas por (a + bi) + (c + di) = (a + c) + (b + d)i e (a + bi)(c + di) = (ac –bd) + (ad + cb)i. O elemento neutro aditivo é (0 + 0i) = 0 e o elemento neutro multiplicativo é (1 + 0i). O inverso aditivo de um elemento (a + bi) é (-a + (-bi)), pois (a + bi) + (-a + (-bi)) = (a – a) + (b – b)i = 0 + 0i = 0.

Definição: Um subconjunto não vazio B de um anel (A, +, •) é dito *subanel de A* se B é um anel com as operações de A.

Proposição**:** Sejam A um anel e B um subconjunto de A. Temos que B é um subanel de A se e somente se são satisfeitas as condições:

(a) A unidade 1 ∈ B;

(b) ∀ a, b ∈ B, a - b ∈ A e ab ∈ B.

Demonstração: (⇒) Se B for um subanel de A, então as condições a) e b) são imediatamente satisfeitas.

(⇐) Suponhamos que as condições (a) e (b) são satisfeitas. Como 1 ∈ B, 0 = 1 – 1 ∈ B. Se x ∈ B, -x = 0 – x ∈ B.

Sejam a, b ∈ B. Como -b ∈ B, logo a + b = a - (-b) ∈ B e como ab ∈ B, podemos concluir que B é um subanel.

Com esta proposição, podemos verificar de uma forma mais eficaz se um determinado subconjunto de um anel é um subanel.

Exemplos: O conjunto ℤ é um subanel do anel ℚ e o conjunto ℤ[2^{1/2}] é um subanel de ℝ.

Definição: Um inteiro gaussiano é um elemento da forma a + bi, em que a, b ∈ ℤ e i² = -1. Chamaremos o conjunto ℤ[i] = { a + bi | a, b ∈ ℤ e i² = -1 } de *Anel dos Inteiros Gaussianos*. O termo Anel é justificado pela seguinte proposição.

Observação: ℤ ⊂ ℤ[i], pois ℤ = { a + 0i | a ∈ ℤ e i² = -1 }. Como a unidade (1 + 0i) = 1 ∈ ℤ e ∀ (a + 0i), (b + 0i) ∈ ℤ, (a + 0i) + (b + 0i) = a + b ∈ ℤ e (a + 0i)(b + 0i) = ab ∈ ℤ, podemos concluir que ℤ é um subanel de ℤ[i].

Resultados

Proposição: O conjunto ℤ[i] é um subanel de ℂ.

Demonstração: (a) A unidade é 1 = 1 + 0i ∈ ℤ[i].

(b) Sejam (a + bi) e (a’ + b’i) ∈ ℤ[i], (a + bi) – (a’ + b’i) = (a + a’) – (b + b’)i ∈ ℤ[i].

(c) (a + bi)(a’ + b’i) = aa’ + ab’i + ba’i + bb’i² = (aa’ – bb’) + (ab’ + a’b)i ∈ ℤ[i].

Define-se por *função norma* em ℂ a seguinte função:

$$N : \mathbb{C} \rightarrow \mathbb{R}^+$$
$$(a + bi) \mapsto |a + bi|^2 = a^2 + b^2$$

Geometricamente, a função norma nos fornece o quadrado do comprimento de um vetor a+bi ∈ ℂ no plano complexo.

Exemplo: N(5 + 3i) = 5² + 3² = 34

Observação: Se z = (a + bi) ∈ ℤ[i], então N(z) = (a² + b²) ∈ ℤ⁺.

Proposição: Se z = (a + bi) e z’ = (a’ + b’i) ∈ ℤ[i], então N(zz’) = N(z)N(z’).

Demonstração: N(zz’) = N((aa’ – bb’) + (ab’ + a’bi) = (aa’ – bb’)² + (ab’ + a’b)² = (aa’)² -2aa’bb’ + (bb’)² + (ab’)² + 2ab’a’b + (a’b)² = (aa’)² + (bb’)² + (ab’)² + (a’b)² = (a² + b²)(a’² + b’²) = N(z)N(z’).

Definição: Seja (A, +, •) um anel. Dizemos que a ∈ A é invertível se existe b ∈ A tal que ab=ba = 1. O elemento b é chamado inverso multiplicativo de a.

Proposição: Seja x = (a + bi) ∈ ℤ[i]. São equivalentes as seguintes afirmações:

(a) x é invertível em ℤ[i];

(b) N(x) = 1;

(c) x ∈ { 1, -1, i, -i }

Demonstração: (a) ⇒(b) Se x é invertível, ∃ x’ ∈ ℤ[i] tal que xx’ = 1. Pela proposição anterior, N(x)N(x’) = N(xx’) = N(1) = 1. Como N(x) e N(x’) ∈ ℤ⁺, segue que N(a) = N(x’) = 1.

(b) ⇒(c) Suponhamos que N(x) = 1. Logo N(x) = N(a + bi) = a² + b² = 1, cujas soluções em ℤ X ℤ são (0, ±1) e (±1, 0). Logo x ∈ { 1, -1, i, -i }.

(c) ⇒(a) É óbvio que todos os elementos do conjunto { 1, -1, i, -i } são invertíveis em ℤ[i].

Definição: Seja (A, +, •) um anel. Dizemos que (A, +, •) é um corpo se todo elemento de A – {0} é invertível e se (A, +, •) não possui divisores de zero, ou seja, ∀ x, y ∈ A com xy = 0 tem-se x = 0 ou y = 0.

Exemplo: O anel (ℚ, +, •) é um corpo, pois para todo a ∈ ℚ-{0}, temos o inverso multiplicativo de a como (1/a), pois ab = 1.

Observamos que o anel ℤ[i] não é um corpo, pois pela proposição anterior, vimos que os únicos elementos de ℤ[i] que são invertíveis são { 1, -1, i, -i}.

Definição: Seja (A, +, •) um anel. Dizemos que A é um anel com divisores de zero se existem a,b ∈ A, ambos não nulos, tais que ab=0. Quando for o caso, a e b são chamados de divisores de zero.

Podemos mostrar que ℤ[i] não possui divisores de zero. De fato, sejam (a + bi), (a’ + b’i) ∈ ℤ[i]. Se (a + bi)(a’ + b’i) = 0 então (aa’ – bb’) + (ab’ + a’b)i = 0. Daí, segue que a = b = 0 ou a’ = b’ = 0.

Problemas

Problema 1. Existe um algoritmo de divisão em ℤ[i], análogo ao existente em ℤ?

Problema 2. Existem formas diferentes (a menos de ordem) de se escrever um inteiro gaussiano?

Referencia Bibliográfica

Abramo Hefez: Curso de Álgebra – Volume 1. SBM, Rio de Janeiro - 1993

* A impressão deste foi financiada pela FAPEG .