Теорія чисел завдання 1

Область цілісності R називається евклідовою областью якщо існує функція(*евклідова норма*)

$$\lambda : R \setminus \{0\} \to \{0, 1, 2, 3, \ldots\}$$

така, що можливе ділення з остачею за нормою меншою ніж дільник. Тобто для кожних $a, b \in R$, $b \neq 0$ існують $q, r \in R$ такі що $a = bq + r$ і або $r = 0$ або $\lambda(r) < \lambda(b)$.

4.

Body of the problem

- Доведіть, що кільце гауссових чисел $R = \mathbb{Z} + \mathbb{Z}\sqrt{-1}$ є евклідовою областю з нормою $\lambda\left(m + n\sqrt{-1}\right) = m^2 + n^2$.

Proof

Покажемо що R є областю цілістності. Нехай $a, b \in R$, $a = a_0 + a_1 i \neq 0$ і $b = b_0 + b_1 i \neq 0$, де $i = \sqrt{-1}$. Тоді

$$\begin{aligned} 0 &= ab \\ &= (a_0 + a_1 i)(b_0 + b_1 i) \\ &= (a_0 b_0 - a_1 b_1) + (a_1 b_0 + a_0 b_1) i \end{aligned}$$

звідки ми отримаємо що

$$\begin{cases} a_0 b_0 - a_1 b_1 = 0 \\ a_1 b_0 + a_0 b_1 = 0 \end{cases}$$

Запишемо систему у матричній формі(якщо розв'язків не буде в $\mathbb{R}$ то їх не буде й в $\mathbb{Z}$)

$$\begin{pmatrix} b_0 \\ b_1 \end{pmatrix} \begin{pmatrix} a_0 & -a_1 \\ a_1 & a_0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

Це матричне рівняння має розв'язок якщо $b_0 = b_1 = 0$ або $a_0^2 + a_1^2 = 0$ що рівносильно $a_0 = a_1 = 0$, але це суперечить припущенню що $ab = 0$, проте $a \neq 0$ і $b \neq 0$ а отже R це область цілістності.

Нехай $\alpha, \beta \in \mathbb{Z}[i]$, $\alpha = a + bi$, $\beta = c + di$, $\beta \neq 0$. Розглянемо добуток $\alpha\beta^{-1}$, так як

$$\beta^{-1} = \frac{c - di}{c^2 + d^2} = \frac{\overline{\beta}}{\lambda(\beta)}$$

то

$$\begin{aligned} \alpha\beta^{-1} &= \frac{(a+bi)(c-di)}{c^2+d^2} \\ &= \frac{1}{c^2+d^2}((ac+bd) + (bc-ad)i) \\ &= \frac{ac+bd}{c^2+d^2} + \frac{bc-ad}{c^2+d^2}i \\ &= (q_1 + r_1) + (q_2 + r_2)i \end{aligned}$$

де $-\frac{1}{2} \leq r_1, r_2 \leq \frac{1}{2}$, $q_1, q_2 \in \mathbb{Z}$. Таке представлення можливе так як ми можемо представити будь-яке раціональне(дійсне) число x у вигляді

$$x = \lfloor x \rfloor + r_1 \quad 0 \leq r_1 \leq \frac{1}{2}$$

або

$$x = \lceil x \rceil + r_2 \qquad -\frac{1}{2} \leq r_2 \leq 0$$

Ми маємо

$$\begin{aligned} \alpha\beta^{-1} &= (q_1 + r_1) + (q_2 + r_2)i \qquad q_1, q_2 \in \mathbb{Z} \quad -\frac{1}{2} \leq r_1, r_2 \leq \frac{1}{2} \\ &= (\underbrace{q_1 + q_2 i}_{\gamma \in \mathbb{Z}[i]}) + (r_1 + r_2 i) \end{aligned}$$

помноживши на β отримаємо

$$\alpha = \beta\gamma + \underbrace{\beta(r_1 + r_2 i)}_{\rho \in \mathbb{Z}[i]}$$

так як $\alpha, \beta\gamma \in \mathbb{Z}[i]$, таким чином $\alpha = \beta\gamma + \rho$, покажемо що $\lambda(\rho) < \lambda(\beta)$

$$\begin{aligned} \lambda(\rho) &= \rho\bar{\rho} \\ &= \beta\bar{\beta}(r_1 + r_2 i)(r_1 - r_2 i) \\ &= \lambda(\beta)(r_1^2 + r_2^2) \leq \frac{1}{2}\lambda(\beta) < \lambda(\beta) \end{aligned}$$

Отже дійсно $\mathbb{Z}[i]$ є Евклідовою областю.

- Покажіть що єдиними оборотними елементами цього кільця є ± 1 та $\pm\sqrt{-1}$, тобто

$$R^{\times} = \{1, -1, \sqrt{-1}, -\sqrt{-1}\}$$

Proof

Нехай a - оборотний елемент в R, тобто існує $b \in R$, такий що $ab = 1$. Таким чином і елемент b буде оборотним в R. Тоді

$$(a_0 + a_1 i)(b_0 + b_1 i) = (a_0 b_0 - a_1 b_1) + (a_0 b_1 + a_1 b_0)i = 1 + 0i$$

отримаємо

$$\begin{cases} a_0 b_0 - a_1 b_1 = 1 \\ a_0 b_1 + a_1 b_0 = 0 \end{cases}$$

у матричному вигляді

$$\begin{pmatrix} b_0 & -b_1 \\ b_1 & b_0 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

Матриця з цілими коефіцієнтами має обернену матрицю з ціл ими коефіцієнтами тоді та тільки тоді коли її визначник дорівнює ± 1. Тоді

$$b_0^2 + b_1^2 = 1 \Rightarrow b_0 = 1 \wedge b_1 = 0 \quad \text{або} \quad b_0 = 0 \wedge b_1 = 1$$

тобто(з доведеного раніше) $b = \pm 1$ або $b = \pm i$.

Далі, помноживши на обернену матрицю, отримаємо

$$\begin{pmatrix} a_0 \\ a_1 \end{pmatrix} = \begin{pmatrix} b_0 & b_1 \\ -b_1 & b_0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} b_0 \\ -b_1 \end{pmatrix}$$

Тобто, знов таки, $a = \pm 1$ або $a = \mp i$. А отже дійсно

$$R^\times = \{\pm 1, \pm i\}$$

- Користуючись алгоритмом Евкліда знайдіть найбільний спільний дільник гауссових чисел $2 + 3\sqrt{-1}$ та $4 + \sqrt{-1}$.

Solution

Так як $17 = \lambda(4 + i) > \lambda(2 + 3i) = 13$, то почнемо алгоритм Евкліда поділивши з залишком $4 + i$ на $2 + 3i$. Для цього потрібно знайти "найближчий" елемент решітки породженої $2 + 3i$. Тоді

$$4 + i = (1 - i)(2 + 3i) - 1$$

Далі

$$2+3i=(-1)(-2-3i)+0$$

Отже $(4+i,2+3i)=-1$, так як найбільший спільний дільник визначається з точністю до множення на оборотний елемент, то $(4+i,2+3i)=1$, а отже $4+i$ та $2+3i$ взаємнопрості.