Цели алгебрични числа.
Определение и примери.

1. Цели алгебрични числа

Дефиниция 1.1. Комплексното число α се нарича *цяло алгебрично число*, когато α е корен на полином с цели коефициенти и старши коефициент 1.

Полином на една променлива със старши коефициент 1 ще наричаме *моничен* полином.

Твърдение 1.1. *Ако едно рационално число $\alpha \in \mathbb{Q}$ е цяло алгебрично число, то α е цяло число.*

Доказателство. Нека

$$\alpha = \frac{a}{b}, \qquad a, b \in \mathbb{Z},$$

където a и b са взаимно прости цели числа и нека

$$f = X^n + a_1 X^{n-1} + \cdots + a_{n-1} X + a_n \in \mathbb{Z}[x]$$

е моничен полином с цели коефициенти, такъв че $f(\alpha) = 0$. Тогава

$$\begin{aligned} a^n &= -(a_1 a^{n-1} b + \cdots + a_{n-1} a b^{n-1} + a_n b^n) \\ &= -b(a_1 a^{n-1} + \cdots + a_{n-1} a b^{n-2} + a_n b^{n-1}). \end{aligned} \tag{1.1}$$

От (1.1) следва, че b дели a^n. Тъй като a^n и b са взаимно прости, то $b = \pm 1$. $\square$

Нека $\alpha_1, \ldots, \alpha_n$ са комплексни числа. Ще означаваме със $\mathbb{Z}[\alpha_1, \ldots, \alpha_n]$ най-малкия подпръстен на $\mathbb{C}$, който съдържа $\mathbb{Z}$ и $\alpha_1, \ldots, \alpha_n$:

$$\mathbb{Z}[\alpha_1, \ldots, \alpha_n] = \{F(\alpha_1, \ldots, \alpha_n) : F \in \mathbb{Z}[X_1, \ldots, X_n]\}.$$

Лема 1.2. *Ако α е цяло алгебрично число, то $\mathbb{Z}[\alpha]$ е крайнопородена абелева група.*

Доказателство. Нека $f \in \mathbb{Z}[X]$ е моничен полином от степен n, такъв че $f(\alpha) = 0$. Ще покажем, че за всяко число $\beta \in \mathbb{Z}[\alpha]$ съществуват цели числа $b_0, b_1, \ldots, b_{n-1} \in \mathbb{Z}$, такива че

$$\beta = b_0 + b_1 \alpha + \cdots + b_{n-1} \alpha^{n-1}. \tag{1.2}$$

Това ще докаже Лема 1.2, защото от (1.2) следва, че абелевата група $\mathbb{Z}[\alpha]$ се поражда от числата $1, \alpha, \ldots, \alpha^{n-1}$.
Нека $F \in \mathbb{Z}[X]$ е полином с цели коефициенти, такъв че $\beta = F(\alpha)$. Тъй като f е моничен полином, то частното q и остатъкът r, които се получават при делението на F с f, са полиноми с цели коефициенти. Нека

$$r = b_0 + b_1 X + \cdots + b_{n-1} X^{n-1}, \text{ където } b_0, b_1, \ldots, b_{n-1} \in \mathbb{Z}.$$

Сега от $F = qf + r$ получаваме

$$\beta = F(\alpha) = q(\alpha) f(\alpha) + r(\alpha) = r(\alpha) = b_0 + b_1 \alpha + \cdots + b_{n-1} \alpha^{n-1}. \qquad \square$$

Твърдение 1.3. *Ако $\alpha_1, \alpha_2, \ldots, \alpha_n$ са цели алгебрични числа то $\mathbb{Z}[\alpha_1, \ldots, \alpha_n]$ е крайнопородена абелева група.*

Доказателство. Нека $n \geq 2$ е естествено число. Да предположим, че пръстените $\mathbb{Z}[\alpha_1, \ldots, \alpha_k]$ са крайнопородени абелеви групи, когато $k < n$ и $\alpha_1, \ldots, \alpha_k$ са цели алгебрични числа. Нека $R = \mathbb{Z}[\alpha_1, \ldots, \alpha_n]$, $S = \mathbb{Z}[\alpha_1, \ldots, \alpha_{n-1}]$ и $T = \mathbb{Z}[\alpha_n]$. Тогава S (съответно T) е крайнопородена абелева група с пораждащи $y_1, \ldots, y_k$ (съответно $z_1, \ldots, z_l$). Освен това всяко число $r \in R$ има представяне

$$r = \sum_{i=1}^{m} s_i t_i, \text{ където } s_i \in R,\ t_i \in T,\ i = 1, \ldots, m.$$

Следователно всяко число $r \in R$ е целочислена линейна комбинация на числата $x_{ij} = y_i z_j \in R$, $i = 1, \ldots, k$, $j = 1, \ldots, l$. Сега Твърдение 1.3 следва от Лема 1.2 и принципа на математическата индукция. □

Както показва следващата важна теорема, обратното твърдение на Твърдение 1.3 също е вярно.

Теорема 1.4. *Ако един пръстен $R \supset \mathbb{Z}$ от комплексни числа е крайнопородена абелева група, то всеки елемент на R е цяло алгебрично число.*

Доказателство. Нека $\alpha \in R$ и нека $x_1, x_2, \ldots, x_n \in R$ е множество от пораждащи елементи на абелевата група A. Да отбележим, че $x_j \neq 0$ за някое $1 \leq j \leq n$, защото $1 \in R$. Тъй като $\alpha x_j \in R$ за всяко $j = 1, \ldots, n$, то съществуват цели числа a_{ij}, $1 \leq i, j \leq n$, такива че

$$\alpha x_j = \sum_{i=1}^{n} a_{ij} x_j, \qquad j = 1, \ldots, n. \tag{1.3}$$

Нека $A \in M_{n \times n}(\mathbb{C})$ е матрицата с коефициенти a_{ij}, $1 \leq i, j \leq n$. Уравнения (1.3) показват, че векторът $0 \neq x = (x_1, x_2, \ldots, x_n) \in \mathbb{C}^n$ е собствен вектор на A със собствена стойност α. Следователно α е корен на характеристичния полином $\chi_A(X)$ на A. Тъй като коефициентите на $\chi_A(X)$ са цели числа (коефициентите на A са цели числа) и старшият коефициент на $\chi_A(X)$ е ± 1, то α е цяло алгебрично число. □

Комбинирайки Твърдение 1.3 и Теорема 1.4 получаваме следната характеризация на целите алгебрични числа:

Твърдение 1.5. *Комплексните числа $\alpha_1, \ldots, \alpha_n$ са цели алгебрични числа тогава и само тогава, когато пръстенът $\mathbb{Z}[\alpha_1, \ldots, \alpha_n]$ е крайнопородена абелева група. Нещо повече, ако $\alpha_1, \ldots, \alpha_n$ са цели алгебрични числа, то всеки елемент на пръстена $\mathbb{Z}[\alpha_1, \ldots, \alpha_n]$ е цяло алгебрично число.*

Доказателство. Следва незабавно от Твърдение 1.3 и Теорема 1.4. □

Теорема 1.6. *Множеството на целите алгебрични числа е подпръстен на $\mathbb{C}$.*

Доказателство. Нека α и β са цели алгебрични числа. Според Твърдение 1.5 всеки елемент на $\mathbb{Z}[\alpha, \beta]$ е цяло алгебрично число. Тъй като $\alpha + \beta,\ \alpha\beta \in \mathbb{Z}[\alpha, \beta]$, те са цели алгебрични числа. Следователно множеството на целите алгебрични числа е подпръстен на $\mathbb{C}$. □

С помоща на следващото твърдение можем да проверим дали дадено алгебрично число е цяло алгебрично число.

Твърдение 1.7. *Алгебричното число $\alpha \in \mathbb{C}$ е цяло алгебрично число тогава и само тогава, когато коефициентите на неговия минимален полином са цели числа.*

Доказателство. Нека

$$q = X^m + b_1 X^{m-1} + \cdots + b_m = (X - \alpha_1)(X - \alpha_2) \dots (X - \alpha_m) \in \mathbb{Q}[X]$$

е минималният полином на алгебричното число $\alpha = \alpha_1$. Ако $q \in \mathbb{Z}[X]$, то α е очевидно цяло алгебрично число.
Обратно, нека α е цяло алгебрично число и нека $f \in \mathbb{Z}[X]$ е моничен полином, такъв че $f(\alpha) = 0$. Тъй като q дели всеки полином $g \in \mathbb{Q}[x]$, такъв че $g(\alpha) = 0$, то q дели f в пръстена $\mathbb{Q}[x]$. Това влече $f(\alpha_i) = 0$ за всички $i = 1, \dots, m$, откъдето следва, че $\alpha_1, \alpha_2, \dots, \alpha_m$ са цели алгебрични числа. Според формулите на Виет $b_1, \dots, b_m \in \mathbb{Z}[\alpha_1, \dots, \alpha_m]$. Следователно $b_1, \dots, b_m$ са също цели алгебрични числа (виж Твърдение 1.5). Но $b_1, \dots, b_m \in \mathbb{Q}$, откъдето $b_1, \dots, b_m \in \mathbb{Z}$, според Твърдение 1.1. □

Нека R е комутативен пръстен. За всеки елемент $a \in R$, ще означаваме с aR главния идеал, който е породен от a в R:

$$aR = \{ar : r \in R\}.$$

Лема 1.8. *Нека R е пръстен от цели алгебрични числа. Ако $a, b, n \in \mathbb{Z}$ са цели числа, такива че*

$$a \equiv b \mod nR,$$

то

$$a \equiv b \mod n\,.$$

Доказателство. Ако $n = 0$, то $a = b$. Ако $n \neq 0$, то от $a - b = nr$ следва, че $r \in \mathbb{Q}$. Тъй като r е цяло алгебрично число, то $r \in \mathbb{Z}$, според Твърдение 1.1. □

2. Примери

Нека $p \in \mathbb{N}$ е просто число. Да припомним, че цялото число a се нарича *квадратичен остатък* (съотв. *квадратичен неостатък*) по модул p, когато сравнението

$$x^2 \equiv a \mod p$$

има решение $x \in \mathbb{Z}$ (съотв. няма решение $x \in \mathbb{Z}$).
Да припомним също, че за всяко $a \in \mathbb{Z}$, което не се дели на p, символът на Льожандър

$$\left(\frac{a}{p}\right) \in \{1, -1\}$$

се дефинира както следва:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{когато } a \text{ е квадратичен остатък по модул } p. \\ -1 & \text{когато } a \text{ е квадратичен неостатък по модул } p. \end{cases}$$

Според добре известният *критерий на Ойлер*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p,$$

когато p е нечетно просто число.

Пример 2.1 (Ферма). Нека $p > 0$ е просто число от вида $4k+1$ в $\mathbb{Z}$. Ще покажем че p е сума на два квадрата на естествени числа. Прилагайки критерия на Ойлер за $a = -1$, получаваме

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \equiv 1 \mod p.$$

Следователно -1 е квадратичен остатък по модул p. Това означава, че съществуват цели числа x и y, такива че

$$py = x^2 + 1 = (1 + xi)(1 - xi).$$

Известно е, че пръстенът на целите гаусови числа $\mathbb{Z}[i]$ е област с еднозначно разлагане на множители. Ако p беше просто число в $\mathbb{Z}[i]$, то p щеше да дели или $1 + xi$ или $1 - xi$, което е невъзможно (p не дели 1). Следователно съществуват цели гаусови числа $z_1 = r_1 + s_1 i$, $z_2 = r_2 + s_2 i$, такива че $|z_1| > 1$, $|z_1| > 1$ и $p = z_1 z_2$. От последното равенство получаваме

$$p^2 = |p|^2 = |z_1|^2 \, |z_2|^2 = (r_1^2 + s_1^2)(r_2^2 + s_2^2). \tag{2.1}$$

Тъй като p е просто число в $\mathbb{Z}$, то от (2.1) следва, че

$$p = r_1^2 + s_1^2 = r_2^2 + s_2^2.$$

Да отбележим, че

$$r_1 = r_2, \qquad s_1 = -s_2,$$

тъй като z_1 и z_2 са комплексно спрегнати.

Пример 2.2. Нека $\omega = \cos\frac{\pi}{4} + i \sin\frac{\pi}{4} = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$ и нека $R = \mathbb{Z}[\omega]$. Тъй като $\omega^4 = -1$, пръстенът R се състои от цели алгебрични числа. Да забележим, че $\sqrt{2} \in R$: $\sqrt{2} = \omega - \omega^3 = \omega + \omega^{-1}$. Ще използуваме аритметиката на R, за да покажем, че за всяко нечетно просто число p

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Да означим $(-1)^{\frac{p^2-1}{8}}$ с $\epsilon(p)$. Лесно се проверява, че

$$\epsilon(p) = \begin{cases} 1 & p \equiv \pm 1 \mod 8, \\ -1 & p \equiv \pm 3 \mod 8. \end{cases}$$

Според критерия на Ойлер

$$\left(\frac{2}{p}\right) \equiv \left(\sqrt{2}\right)^{p-1} \mod p\,,$$

откъдето

$$\sqrt{2}\left(\frac{2}{p}\right) \equiv \left(\sqrt{2}\right)^{p} \mod pR\,.$$

Сега

$$\left(\sqrt{2}\right)^{p} = (\omega + \omega^{-1})^p \equiv \omega^p + \omega^{-p} = 2\cos\frac{p\pi}{4} \mod pR\,.$$

Непосредствено се вижда, че $2\cos\frac{p\pi}{4} = \epsilon(p)\sqrt{2}$, откъдето

$$\sqrt{2}\left(\frac{2}{p}\right) \equiv \epsilon(p)\sqrt{2} \mod pR\,. \tag{2.2}$$

Умножавайки сравнение (2.2) по $\sqrt{2}$, получаваме

$$2\left(\frac{2}{p}\right) \equiv 2\,\epsilon(p) \mod pR\,. \tag{2.3}$$

Съгласно Лема 1.8, сравнение (2.3) влече

$$2\left(\frac{2}{p}\right) \equiv 2\,\epsilon(p) \mod p\,.$$

Окончателно

$$\left(\frac{2}{p}\right) = \epsilon(p)$$

защото p е нечетно просто число.