

数チャレ 第18回 (2002年7月)

i を虚数単位とし、複素整数の集合

$$G = \{a + bi \mid a, b \text{ は整数}\}$$

において、通常の整数と同じように倍数、約数の概念を定義する：

$$\alpha \in G \text{ が } \beta \in G \text{ の倍数} \iff \alpha = \beta\gamma \text{ となる } \gamma \in G \text{ が存在}$$

$$\alpha \in G \text{ が } \beta \in G \text{ の約数} \iff \alpha\gamma = \beta \text{ となる } \gamma \in G \text{ が存在}$$

G において、1の約数を(G の)単元という。 G の要素 $\pi = p + qi$ (p, q は実数)が $|\pi|^2 = p^2 + q^2 \geq 2$ であり、 $\pi\varepsilon$ (ε は G の単元)以外の約数をもたないとき、 π を(G の)素元という。また、素元と単元の積は素元である。

- (1) G の単元をすべて求めよ。
- (2) 単元でない G の任意の要素は、有限個の素元の積で表されることを示せ。
- (3) 素数 p が $p \equiv 1 \pmod{4}$ を満たすとき、 $m^2 + 1$ が p で割り切れるような自然数 m が存在することを示し、 p は G において素元でないことを示せ。
- (4) $p \equiv 1 \pmod{4}$ を満たす素数 p は、ある自然数 a, b を用いて
$$p = a^2 + b^2$$
 と表されることを示せ。

コメント：(3)を示す際には、6月の問題で証明したウィルソンの定理を用いてよい。

解答

- (1) $\varepsilon = a + bi$ を G の単元とすると、ある整数 c, d が存在して

$$(a + bi)(c + di) = 1$$

を満たす。両辺の絶対値の平方を考えると

$$(a^2 + b^2)(c^2 + d^2) = 1$$

$a^2 + b^2, c^2 + d^2$ はともに正の整数であるから

$$a^2 + b^2 = c^2 + d^2 = 1$$

$$\therefore (a, b) = (1, 0), (-1, 0), (0, 1), (0, -1)$$

$$\therefore \varepsilon = \pm 1, \pm i \quad (\text{答})$$

- (2) 有限個の素元の積で表せない G の元が存在すると、その中で絶対値が最小のものが存在するはずであり、それを α とする。 α の定め方により α 自身は素元ではないから、

$$\alpha = \beta\gamma, \quad |\beta| > 1, \quad |\gamma| > 1$$

を満たす G の元 β, γ が存在する。

$$|\beta| < |\beta||\gamma| = |\alpha|, \quad |\gamma| < |\beta||\gamma| = |\alpha|$$

であるから、 $|\alpha|$ の最小性より β, γ はともに有限個の素元の積で表される。すると、 α も有限個の素元の積で表されることになり、 α の定め方に反してしまう。

したがって、 G の任意の要素は有限個の素元の積で表される。 (証明おわり)

(3) $p = 4n + 1$ (n は自然数) と表されるならば,

$$(p-1)! = (p-1)(p-2)(p-3)\cdots(p-2n) \times (2n)! \\ \equiv \{(2n)!\}^2 \pmod{p}$$

ウィルソンの定理より $(p-1)! \equiv -1 \pmod{p}$ であるから,

$$m = (2n)!, \quad m^2 + 1 \equiv 0 \pmod{p}$$

p が G において素元であるとすれば, (通常の整数と同様に)

$$p(a+bi) = m+i \quad \text{または} \quad p(a+bi) = m-i$$

となる整数 a, b が存在することになるが, 虚部を比べれば p が (通常の整数において) 1 の約数となって矛盾する。

よって, p は G において素元ではない。 (証明おわり)

(4) (2), (3) より, p は G において 2 個以上の素元の積

$$p = \pi_1 \pi_2 \cdots \pi_n \quad \dots\dots \textcircled{1}$$

と表される。両辺の複素共役をとると

$$p = \bar{\pi}_1 \bar{\pi}_2 \cdots \bar{\pi}_n \quad \dots\dots \textcircled{2}$$

となるから, 辺々かけあわせて

$$p^2 = |\pi_1|^2 |\pi_2|^2 \cdots |\pi_n|^2 \quad \dots\dots \textcircled{3}$$

$|\pi_1|^2, |\pi_2|^2, \dots, |\pi_n|^2$ はいずれも整数であるから, 素数の性質より

p は 1 つの $|\pi_k|^2$ だけを割り切る

が, ③および $n \geq 2$ より $n = 2$ となり, ①, ②より

$$p = \pi_1 \pi_2 = \bar{\pi}_1 \bar{\pi}_2$$

となる。

$\pi_1 = a + bi$ ($a, b \in \mathbb{Z}$) とおく。

a と b の (通常の整数における) 最大公約数を d とすると, $p = \pi_1 \pi_2$ の実部を比べて d は p の約数であることがわかるから, $d = 1$ または $d = p$ である。 $d = p$ ならば $|\pi_1|^2 \geq p, |\pi_2|^2 > 1$ より $p^2 = |\pi_1|^2 |\pi_2|^2$ に反するから,

a と b は (通常の整数として) 互いに素

である。

$$\pi_2 = \frac{p}{a+bi} = \frac{p(a-bi)}{(a+bi)(a-bi)} = \frac{ap}{a^2+b^2} - \frac{bp}{a^2+b^2}i$$

は G の要素であるから, $a^2 + b^2$ は ap と bp の公約数である。

a と b は互いに素であるから $a^2 + b^2$ は p の約数であり,

$$a^2 + b^2 = 1 \quad \text{または} \quad a^2 + b^2 = p$$

である。 $a^2 + b^2 = |\pi_1|^2 > 1$ より

$$p = a^2 + b^2$$

(証明おわり)