代数数理工学

國廣昇教員

2008/07/23

1. n を自然数とする. 集合 Z_n を $Z_n = \{0, 1, \cdots, n-1\}$ で定義する. 代数系 $(Z_n, \times_n)$ を考える. ここで, 算法 $\times_n$ は, $a, b \in Z_n$ に対して, $a \times b \mod n$ とする. ここで, $\mod n$ は n での剰余を意味する. Z_n から Z_n への写像 f を $f(x) = x \times_n x$ と定義する. 以下の問に答えよ.
   (a) f は準同型写像であることを示せ.
   (b) $x, y \in Z_n$ に対して, $f(x) = f(y)$ のとき, $x \approx y$ と定義する. このとき, $\approx$ は同値関係となることを示せ.
   (c) さらに, $\approx$ は, Z_n の算法 $\times_n$ と両立することを示せ.
   (d) n を異なる二つの素数 p, q の積とする. 集合 $A(a) = \{x \in Z_n | x \approx a\}$ と定義する. このとき, $A(a)$ は,
   $$\{a, n-a, a', n-a'\} \subseteq A(a)$$
   を満たすことを示せ. ただし, a' は, $a' = a \mod p, a' = -a \mod q$ を満たす Z_n の要素である.

2. E を体 F の拡大体とし, α を E の元とする. このとき, 次で与えられる集合 J_α を考える.
   $$J_\alpha = \{f(X) \in F[x] | f(\alpha) = 0\}$$
   このとき, 以下の問に答えよ.
   (a) J_α は $F[X]$ と同じ算法の下で, 可換群となることを証明せよ.
   (b) J_α は, $F[X]$ のイデアルとなることを示せ.

3. 72 の約数の集合を E とおく. 任意の $a, b \in E$ に対し, 算法 $\cap, \cup$ を次のように定義する.
   $$\mathrm{lcm}(a, b) = a \cap b, \ \gcd(a, b) = a \cup b$$
   このとき, 以下の問に答えよ.
   (a) $(E, \cap, \cup)$ に対する Hasse 図を書け.
   (b) 任意の $a, b \in E$ に対して, 2 つの商束 $(a \cup b)/a, b/(a \cap b)$ は同型であることを示せ.

4. 以下の問に答えよ.
   (a) $f(x) = x^3 + x + 1$ は, $Z_2[X]$ 上の既約多項式となることを示せ.
   (b) $Z_2[X]/(f(x))$ は体となる. 実際に $+$ と $\cdot$ に関する演算表を作り, 体となることを確認せよ. 自明な箇所に関しては, 適当に省略してよい.
   (c) 自然数 i, j に対して, x^i と x^j を $f(x)$ で割った余りは, $i \neq j \mod 7$ であるとき, 異なることを証明せよ.