代数学２，第１回の内容の理解度チェックの解答

2025/4/14　担当：那須

$\boxed{1}$ 次の環 R と $a, b \in R$ に対し和 $a+b$ および積 ab を計算せよ．

(1) $R = \mathbb{Z}[x]$, $a = 3x+2$, $b = 2x^2 - x + 5$

(2) $R = \mathbb{Q}[x]$, $a = \frac{1}{2}x + 1$, $b = 3x - 2$

(3) $R = \mathbb{Z}/15\mathbb{Z}$, $a = 8$, $b = 10$

(**解答**)

(1) $a+b = (3x+2) + (2x^2 - x + 5) = 2x^2 + 2x + 7$,
$ab = (3x+2)(2x^2 - x + 5) = 6x^3 + x^2 + 13x + 10$.

(2) $a+b = (\frac{1}{2}x - 1) + (3x-2) = \frac{7}{2}x - 1$, $ab = (\frac{1}{2}x - 1)(3x-2) = \frac{3}{2}x^2 + 2x - 2$.

(3) $a+b = 8 + 10 = 18 = 3$, $ab = 8 \cdot 10 = 8 \cdot (-5) = -40 = 5$.

$\boxed{2}$ p を素数とするとき，

$$x^p \equiv x \pmod{p}$$

がすべての整数 x について成り立つことを示せ (フェルマーの定理).

(**解答**)　まず $x = n \geq 0$ の場合に数学的帰納法により証明する．$n = 0$ のときは両辺とも 0 に等しく明らかである．整数 a, b に対し，

$$(a+b)^p \equiv a^p + b^p \pmod{p}$$

が成り立つことを思い出す．このことから

$$n^p = ((n-1)+1)^p \equiv (n-1)^p + 1^p$$

が成り立つ．したがって $x = n-1$ まで正しいと仮定すると，

$$n^p \equiv (n-1) + 1 = n$$

となり $x = n$ のときも正しい．$x = -n$ $(n > 0)$ のときは，

$$x^p = (-n)^p = (-1)^p n^p \equiv (-1)^p n = -n = x \pmod{p}$$

より従う[1].

[1] $p = 2$ のとき $(-1)^2 = 1 \equiv -1 \pmod{p}$ となることに注意せよ．

$\boxed{3}$ 実数を成分とする n 次正方行列全体の集合

$$M(n,\mathbb{R}) = \left\{ A = (a_{ij}) \mid a_{ij} \in \mathbb{R}, 1 \leq i,j \leq n \right\}$$

が行列の和と積に関して, 環になることを確認せよ. またこの環の単元は何か答えよ. ただし行列の和と積に関する性質 (分配法則等) は改めて証明しなくて良い.

(**解答**)

(1) (**和に関して可換群になること**) $A,B,C \in M(n,\mathbb{R})$ とする. 和に関し

$$(A+B)+C = A+(B+C)$$

が成り立ち, 結合法則が満たされる. 零行列 $O \in M(n,\mathbb{R})$ が存在し, 任意の $A \in M(n,\mathbb{R})$ に対し,

$$A + O = O + A = A$$

が成り立つので, O は $M(n,\mathbb{R})$ の加法に関する単位元である. また, 任意の $A \in M(n,\mathbb{R})$ に対し, $-A = (-1)A$ を考えれば

$$A + (-A) = (-A) + A = O$$

を満たし, $-A$ は A の加法逆元となる. 明らかに $A+B = B+A$, $(A, B \in M(n,\mathbb{R}))$ が成り立つ. したがって, $M(n,\mathbb{R})$ は加法に関して可換群となる.

(2) (**結合法則**) 行列の積に関する結合法則により, 任意の $A,B,C \in M(n,\mathbb{R})$ に対し,

$$A(BC) = (AB)C$$

が成り立つ.

(3) (**分配法則**) 行列の積に関する分配法則により, 任意の $A,B,C \in M(n,\mathbb{R})$ に対し,

$$A(B+C) = AB + AC, \qquad (A+B)\cdot C = AC + BC$$

が成立する.

以上により $M(n,\mathbb{R})$ は環になる. 単位行列 E はこの環の単位元であるから, A の逆行列 A^{-1}, すなわち

$$A \cdot A^{-1} = A^{-1}A = E$$

を満たす行列 A^{-1} は A の乗法逆元である. したがって $M(n,\mathbb{R})$ の単元は正則行列全体となる.

[1]※この講義に関する情報はホームページを参照. https://hirokazunasu.github.io/2025/alg2.html