

情報数学 II 演習問題 (12)

番号：

氏名：

1 $f(x) = x^2 + 1$ によって構成される有限体 $GF(3^2)$ に関する以下の問いに答えよ.

- (1) 上の $GF(3^2)$ 上において, $(a+1)^k$ を $k = 1, 2, \dots, 8$ について計算し, $a+1$ が $GF(3^2)$ の原始根と呼べるかどうか, 判別せよ.
- (2) 上の $GF(3^2)$ 上において, a^k を $k = 1, 2, \dots, 8$ について計算し, a が $GF(3^2)$ の原始根と呼べるかどうか, 判別せよ.
- (3) a の $GF(3)$ 上の最小多項式を求めよ.
- (4) $a+1$ の $GF(3)$ 上の最小多項式を求めよ.
- (5) 上問 (3), (4) で求めた最小多項式が原始多項式と言えるか, 理由を明らかにして判別せよ.

2 $f(x) = x^2 + x + 1$ は既約多項式であり, 有限体 $GF(2^2)$ を構成する. この有限体に関する以下の問いに答えよ.

- (1) a は $GF(2^2)$ 上の原始根といえるか. 理由を明らかにして判定せよ.
- (2) 1 の $GF(2^2)$ 上の最小多項式を求めよ.
- (3) a の $GF(2^2)$ 上の最小多項式を求めよ.
- (4) この $GF(2^2)$ 上の原始多項式をすべて求めよ.