位数 q の有限体を $\mathbb{F}_q$ と表す。($\mathbb{F}_q$ を $GF(q)$ と書くこともある。)

Galois field の略

資料10-3

$\boxed{\text{問題 10-0}}$ 問題5-1 ～5-3 および問題9-1 について復習せよ。 □

$\boxed{\text{問題 5-1}}$ K は標数 0 の体であるとし，L はその任意の拡大体であるとする。K 上の既約多項式が L の中に重根を持たないことを示せ。 □

$\boxed{\text{問題 5-2}}$ 正標数の体の標数が常に素数になることを示せ。 □

$\boxed{\text{問題 5-3}}$ p は素数であるとし，$L = \mathbb{F}_p(t) =$ (1変数 t の $\mathbb{F}_p$ 上の有理函数体) とおく。L の部分体 K と K 上の既約多項式 $F(x) \in K[x]$ の組 $(K, F(x))$ で $F(x)$ が L の中に重根を持つものの1つを具体的に構成せよ。 □

$L = \mathbb{F}_p(t)$, $K = \mathbb{F}_p(t^p)$, $F(x) = x^p - t^p \in K[x]$ が例になっている。
(これは純非分離拡大の典型例になっている。)

問題9-1については資料10-1で解説した： $\overline{\mathbb{F}_p} = \bigcup_{n=1}^{\infty} \mathbb{F}_{p^n}$ ($\mathbb{F}_p$ の代数閉包)。

$\boxed{\text{問題 10-1}}$ $p=17, 23, 41$ について $\mathbb{F}_p^\times = \langle a \rangle$ をみたす $a \in \mathbb{F}_p^\times$ を求めよ. □

$\boxed{\text{例}}$ $\mathbb{F}_7 = \{0,1,2,3,4,5,6\}$ と書くと, 　$\bar{0}, \bar{1}, \dots, \bar{6}$ と書くべきだが, てぬきして単に $0, 1, \dots, 6$ と書いた.

$\underline{2} \neq 1$, $2^2 = \underline{4} \neq 1$, $2^3 = \underline{1}$ なので $\langle 2 \rangle \subsetneq \mathbb{F}_7^\times$. 　(次に $1, 2, 4$ 以外を調べる.)

$\underline{3} \neq 1$, $3^2 = \underline{2} \neq 1$, $3^3 = \underline{6} \neq 1$, $3^4 = \underline{4} \neq 1$, $3^5 = \underline{5} \neq 1$, $3^6 = \underline{1}$ なので $\mathbb{F}_7^\times = \langle 3 \rangle$. □

$\boxed{\text{問題 10-2}}$ K は標数 p の体で $a, b \in K$ であるとし,

$x^p - a$ と $x^p - x - b$ は K 上既約であると仮定し,

L, M をそれぞれの K 上での最小分解体であるとする.

L と M が体 K 上で同型になることはあるか? □

$\boxed{\text{問題 10-3}}$ 有限体の有限次拡大が単拡大になることを示せ. □

(有限体 K とその有限次拡大 L に対して, ある $\theta \in L$ が存在して $L = K(\theta)$ となることを示せ.)

$\boxed{\text{問題 10-4}}$ k は標数 p の体であるとし, $L = k(s, t)$, $K = k(s^p, t^p)$ とおく. 　s と t は文字

このとき, 拡大 L/K について, $[L:K] = p^2$ で L が K の単拡大にならないことを示せ.

ここで, $k(s,t)$ は体 K 上の 2 変数有理函数体である. (cf. 問題 5-3) □