$\boxed{\text{問題 9-1}}$ ($\mathbb{F}_p$ の代数閉包)

p は素数であるとし, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ とおく. $\mathbb{F}_p$ は位数 p で標数 p の有限体になる.

Ω は代数閉体であるような $\mathbb{F}_p$ の拡大体であるとする.　$\mathbb{F}_p = \{0, 1, \dots, p-1\}$ と書く.

(そのような Ω の存在は Steinitz の定理によって保証される.) 以下を示せ:

(1) Ω の任意の部分体 K は $\mathbb{F}_p$ を含む.

(2) $n = 1, 2, 3, \dots$ について, $F_n(x) = x^{p^n} - x \in \mathbb{F}_p[x]$ とおき,

Ω における $F_n(x)$ の根全体を $L_n = \{\alpha \in \Omega \mid F_n(\alpha) = 0\}$ と書く.

このとき, L_n は Ω に含まれる唯一つの位数 p^n の有限部分体になる.

以下, $\mathbb{F}_{p^n} = L_n$ とおく.

(3) $m \mid n$ のとき, $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$

(4) $L_\infty = \bigcup_{n=1}^{\infty} \mathbb{F}_{p^n}$ とおく. L_∞ は $\mathbb{F}_p$ の代数閉包になる.

(5) $e, n \in \mathbb{Z}_{>0}$, $q = p^e$ とし, $\mathbb{F}_{q^n}$ の $\mathbb{F}_q$ 上の Frobenius 自己同型 F を $F(\gamma) = \gamma^q$ ($\gamma \in \mathbb{F}_{q^n}$) と定める.

$\mathbb{F}_{q^n}$ は $\mathbb{F}_q$ の n 次の Galois 拡大で $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) = \langle F \rangle \cong C_n$. □

$\boxed{\text{解答例}}$ (1) K は Ω の部分体であるとする. $0, 1 \in K$ で, $2 = 1+1$, $3 = 1+1+1, \dots$, $p-1 = \overbrace{1 + \cdots + 1}^{p-1\text{個}}$ も

$0 = 0_K$　$1 = 1_K$

K の元になるので $\mathbb{F}_p = \{0, 1, \dots, p-1\} \subset K$.

注 $2, 3, \dots, p-1$ の K での像も同じ記号で書いてしまっていることに注意. (手ぬき)

(2) $\boxed{1}$ L_nがΩの部分体になることを示そう。

$\alpha, \beta \in L_n$と仮定する。$0, 1, \alpha+\beta, -\alpha, \alpha\beta \in L_n$かつ$\alpha \neq 0$のとき$\alpha^{-1} \in L_n$となることを示せばよい。標数$p$の世界なので$(a+b)^p = a^p + b^p$が成立している。

$F_n(0) = 0^{p^n} - 0 = 0$ なので $0 \in L_n$.

$F_n(1) = 1^{p^n} - 1 = 0$ なので $1 \in L_n$

$F_n(\alpha+\beta) = (\alpha+\beta)^{p^n} - (\alpha+\beta) = \alpha^{p^n} + \beta^{p^n} - (\alpha+\beta) = F_n(\alpha) + F_n(\beta) = 0+0 = 0$.

ゆえに$\alpha+\beta \in L_n$.

$$F_n(-\alpha) = (-\alpha)^{p^n} - (-\alpha) = \begin{cases} p=2\text{のとき } -\alpha=\alpha \text{ なので } \alpha^{p^n} - \alpha = F_n(\alpha) = 0, \\ p\text{が奇数のとき } -\alpha^{p^n} + \alpha = -F_n(\alpha) = 0. \end{cases}$$

ゆえに$-\alpha \in L_n$.

αまたはβが0ならば$\alpha\beta = 0 \in L_n$は自明なので$\alpha \neq 0, \beta \neq 0$と仮定する。

α, βは$F_n(x) = x^{p^n} - x = x(x^{p^n-1} - 1)$の$0$でない根なので$x^{p^n-1} - 1$の根になるので、$F_n(\alpha\beta) = \alpha\beta\left((\alpha\beta)^{p^n-1} - 1\right) = \alpha\beta\left(\underbrace{\alpha^{p^n-1}}_{=1}\underbrace{\beta^{p^n-1}}_{=1} - 1\right) = 0$.

ゆえに、$\alpha\beta \in L_n$.

さらに、$\alpha \neq 0$のとき、$F_n(\alpha^{-1}) = \alpha^{-1}\left((\alpha^{-1})^{p^n-1} - 1\right) = \alpha^{-1}\left((\underbrace{\alpha^{p^n-1}}_{=1})^{-1} - 1\right) = 0$

なので$\alpha^{-1} \in L_n$.

$\boxed{2}$ $|L_n| = p^n$ を示そう。

$F_n(x) = x^{p^n} - x \in \mathbb{F}_p[x]$ が重根を持たないことを示せばよい。

$F_n'(x) = -1$ なので $F_n(x)$ と $F_n'(x)$ の共通根は存在しない。 ← $(x^{p^n})' = \underbrace{p^n}_{=0}\, x^{p^n-1}$ (標数がp)

ゆえに、$F_n(x)$ は重根を持たない。

$\boxed{3}$ K を Ω の位数 p^n の部分体とすると、$K = L_n$ となることを示そう。

$0 \in K$ は $F_n(x) = x(x^{p^n-1} - 1)$ の根であり、$K^\times$ は位数 $p^n - 1$ の有限群になるので、

任意の $\alpha \in K^\times$ は $\alpha^{p^n-1} = 1$ をみたし、$F_n(x)$ の根になる

ゆえに、$K \subset L_n$。 $|K| = p^n = |L_n|$ なので $K = L_n$。

以下、$\mathbb{F}_{p^n} = L_n$ とおく。 位数p^n (元の個数がp^n) の有限体を $\mathbb{F}_{p^n}$ と書く。

(3) $m|n$ のとき、$n = lm$ と書くと、

$$p^n - 1 = p^{lm} - 1 = (p^m)^l - 1 = \underbrace{(p^m-1)}_{=:M\text{ とおく}}\underbrace{(p^{m(l-1)} + p^{m(l-2)} + \cdots + p^m + 1)}_{=:N\text{ とおく。}}$$

$x^{K}-1 = (x-1)(x^{K-1}+x^{K-2}+\cdots+1)$

$$F_n(x) = x(x^{p^n-1} - 1) = x(x^{MN} - 1) = x(x^M - 1)(x^{M(N-1)} + x^{M(N-2)} + \cdots + x^M + 1)$$

$$= F_m(x)(x^{M(N-1)} + \cdots + x^M + 1).$$

ゆえに、$F_m(x)$ の根は $F_n(x)$ の根になるので $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$。

(4) $\boxed{1}$ $\alpha, \beta \in L_\infty$ に対して，ある m, n で $\alpha \in \mathbb{F}_{p^m}$，$\beta \in \mathbb{F}_{p^n}$ となるものが存在する．
(3)より，$\mathbb{F}_{p^m} \subset \mathbb{F}_{p^{mn}} \supset \mathbb{F}_{p^n}$ なので $\alpha, \beta \in \mathbb{F}_{p^{mn}}$，$\alpha+\beta, -\alpha, \alpha\beta \in \mathbb{F}_{p^{mn}} \subset L_\infty$ となる．
$\alpha \neq 0$ なら $\alpha^{-1} \in \mathbb{F}_{p^{mn}} \subset L_\infty$．これより，$L_\infty$ が Ω の部分体になることがわかる．

$\boxed{2}$ $\mathbb{F}_{p^n} = L_n$ の元は $F_n(x) \in \mathbb{F}_p[x]$ の根なので $\mathbb{F}_p$ 上代数的である．
ゆえに，$L_\infty = \bigcup_{n=1}^{\infty} \mathbb{F}_{p^n}$ のすべての元は $\mathbb{F}_p$ 上代数的である．

$\boxed{3}$ $\alpha \in \Omega$ を $\mathbb{F}_p$ 上代数的な元とする．
L_∞ が $\mathbb{F}_p$ の代数閉包であることを示すには $\alpha \in L_\infty$ を示せばよい．

$L = \mathbb{F}_p(\alpha)$，$n = [L : \mathbb{F}_p]$ とおくと，L は $\mathbb{F}_p$ 上 n 次元のベクトル空間
になるので $|L| = p^n$ なので，L は Ω の位数 p^n の有限部分体である．
(2)より $L = L_n = \mathbb{F}_{p^n} \subset L_\infty$ となる．これより $\alpha \in L_\infty$ が得られる．

(5) $q=p^e$, $e,n\in\mathbb{Z}_{>0}$, $F(\gamma)=\gamma^q$ $(\gamma\in\mathbb{F}_{q^n})$ とする.

$\mathbb{F}_q$の有限次拡大がn次拡大であることと元の個数がq^nであることは同値なので

$\mathbb{F}_{q^n}$は$\mathbb{F}_q$のn次拡大になる.

(2)より, $\mathbb{F}_{q^n}=\{\alpha\in\Omega \mid x^{q^n}-x=0\}$となる.

ゆえに, $\mathbb{F}_{q^n}$は重根を持たない$x^{q^n}-x\in\mathbb{F}_q[x]$の$\mathbb{F}_q$上での最小分解体なので

$\mathbb{F}_{q^n}$は$\mathbb{F}_q$のGalois拡大になる.

Galois理論の一般論より, $|\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)|=[\mathbb{F}_{q^n}:\mathbb{F}_q]=n$.

$\mathbb{F}_{q^n}^\times$は巡回群になるのでその生成元αをとれる. αの位数はq^n-1になるので,

α, $F(\alpha)=\alpha^q$, $F^2(\alpha)=\alpha^{q^2}$, $\dots$, $F^{n-1}(\alpha)=\alpha^{q^{n-1}}$は互いに異なり, $F^n(\alpha)=\alpha^{q^n}=\alpha$となる.

特に$1, F, F^2, \dots, F^{n-1}$は互いに異なるので,

$\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)=\{1,F,\dots,F^{n-1}\}=\langle F\rangle\cong C_n$となる

□

$\boxed{\text{問題 9-2}}$ Artinの定理（資料08-2を見よ）を認めて以下を示せ。

（注 有理式 $=$ 有理函数）

k は体であるとし，$L = k(t_1, \dots, t_n)$ は体 k 上の n 変数有理函数体であるとする。$t_1, \dots, t_n$ の基本対称式 $e_1, \dots, e_n$ を次のように定める：

$$e_r = \sum_{1 \leqq i_1 < \cdots < i_r \leqq n} t_{i_1} \cdots t_{i_r}. \quad \leftarrow \binom{n}{r} \text{項の式.}$$

たとえば，$n=3$ のとき，

$$e_1 = t_1 + t_2 + t_3, \quad e_2 = t_1 t_2 + t_1 t_3 + t_2 t_3, \quad e_3 = t_1 t_2 t_3.$$

L の部分体 K を $K = k(e_1, \dots, e_n)$ と定める。以下を示せ。

(1) L は $F(x) = x^n + \sum_{r=1}^{n} (-1)^r e_r x^{n-r} \in K[x]$ の K 上での最小分解体である。

(2) $[L : K] = n!$

(3) $\mathrm{Gal}(L/K) \cong S_n$. □

$\boxed{\text{解答例}}$ (1)

$$\prod_{i=1}^{n} (x - t_i) = x^n + \sum_{r=1}^{n} \underbrace{\sum_{1 \leqq i_1 < \cdots < i_r \leqq n} (-t_{i_1}) \cdots (-t_{i_r})}_{= (-1)^r e_r} x^{n-r} = F(x).$$

ゆえに，$F(x)$ の根の全体は $t_1, \dots, t_n$ になる。

$L \supset K(t_1, \dots, t_n) \supset k(t_1, \dots, t_n) = L$ より，$L = K(t_1, \dots, t_n)$.

これで，L が $F(x)$ の K 上での最小分解体であることがわかった。

(2)と(3)を示そう。

$\boxed{1}$ S_n の L への作用を、$\sigma \in S_n$ と $f(t_1, \dots, t_n) \in L = k(t_1, \dots, t_n)$ について
$\sigma(f(t_1, \dots, t_n)) = f(t_{\sigma(1)}, \dots, t_{\sigma(n)})$ と定めることができる。
各 $\sigma \in S_n$ の作用は L の体の自己同型になっている。
これによって、L の自己同型群の部分群 G で S_n と同型なものが得られた。
$K' = L^G = \{\alpha \in L \mid \sigma(\alpha) = \alpha \ (\forall \sigma \in G \cong S_n)\}$ とおくと、
Artinの定理より、L/K' は有限次Galois拡大で、

$$\mathrm{Gal}(L/K') = G \cong S_n, \qquad [L:K'] = |G| = n!$$

ゆえに、$K = K'$ を示せば(2), (3)が示されたことになる。

$\boxed{2}$ $\sigma \in S_n$ について、$\sigma(e_r) = e_r$ (e_r は対称式)なので、$e_1, \dots, e_n \in K'$。
$k \subset K'$ でもあるので $K = k(e_1, \dots, e_n) \subset K'$ で $[L:K] \geqq [L:K'] = n!$

この逆向きの不等式を示したい。

3 $t_1, t_2, \dots, t_m$ の基本対称式を $e'_1, \dots, e'_m$ と書き，
$t_{m+1}, t_{m+2}, \dots, t_n$ の基本対称式を $e''_1, \dots, e''_{n-m}$ と書き，
$e'_{r'} = 0 \ (r' > m)$，$e''_{r''} = 0 \ (r'' > n-m)$ と約束しておく．

$$\prod_{i=1}^{m}(x - t_i) \times \prod_{i=m+1}^{n}(x - t_i) = \prod_{i=1}^{n}(x - t_i)$$ より

$$\left(x^m + \sum_{r'=1}^{m}(-1)^{r'} e'_{r'} x^{m-r'}\right)\left(x^{n-m} + \sum_{r''=1}^{n-m}(-1)^{r''} e''_{r''} x^{n-m-r''}\right) = x^n + \sum_{r=1}^{n}(-1)^r e_r x^{n-r}.$$

ゆえに
$$\begin{cases} e''_1 + e'_1 = e_1 \\ e''_2 + e'_1 e''_1 + e'_2 = e_2 \\ e''_3 + e'_1 e''_2 + e'_2 e''_1 + e'_3 = e_3 \\ \cdots\cdots\cdots \\ e''_{n-m} + e'_1 e''_{n-m-1} + e'_2 e''_{n-m-2} + \cdots = e_{n-m} \end{cases}$$

ピンとこない人は
$n=7$，$m=3$ の場合に
確認してみよ．

これは上から順に $e''_1, e''_2, \dots$ について解けて，$e''_1, \dots, e''_{n-m}$ が
e_r と $e'_{r'}$ たちの多項式で書けることがわかる．

$\boxed{4}$ $L_m = K(t_1, \dots, t_m)$ $(m=1, \dots, n)$, $L_0 = K$ とおく。このとき、

$$L_{m+1} = L_m(t_{m+1}), \quad K = L_0 \subset L_1 \subset \cdots \subset L_n = L.$$

$\boxed{5}$ さらに $\boxed{3}$ より、$e''_1, \dots, e''_{n-m} \in K(e'_1, \dots, e'_m) \subset K(t_1, \dots, t_m) = L_m$ であり、

$F_m(x) = (x - t_{m+1})(x - t_{m+2}) \cdots (x - t_n)$ $(m = 0, 1, \dots, n-1)$ とおくと、

$$F_m(x) = x^{n-m} + \sum_{r''=1}^{n-m} (-1)^{r''} e''_{r''} x^{n-m-r''} \in L_m[x].$$

$\deg F_m(x) = n-m$

$\boxed{6}$ t_{m+1} は $F_m(x)$ の根なので $[L_{m+1} : L_m] = [L_m(t_{m+1}) : L_m] \leqq n-m$.

$\boxed{7}$ ゆえに、$[L:K] = \underbrace{[L_n : L_{n-1}]}_{\leqq 1} \cdots \underbrace{[L_2 : L_1]}_{\leqq n-1} \underbrace{[L_1 : L_0]}_{\leqq n} \leqq n!$

$m=n-1$　$m=1$　$m=0$

$\boxed{2}$ の逆向きの不等式!

$\boxed{8}$ これと $\boxed{2}$ を合わせると、$K = K'$ が得られる。

$\to K \subset K'$, $[L:K] \geqq [L:K'] = n!$

$\boxed{\text{q.e.d.}}$