問 13–1. 素数 p と $1 \leq k \leq p-1$ とに対し、$p \mid \binom{p}{k}$ である。

問 13–2. K を標数 $p > 0$ の体とするとき、$a, b \in K$ に対し、$(a+b)^p = a^p + b^p, (ab)^p = a^p b^p$ となる。即ち、$\varphi : K \to K; a \mapsto a^p$: (中への) 体同型。

問 13–3. (再掲) 素数 p と自然数 r との組 (p, r) で $q := p^r \leq 10$ なるもの $(p, r) = (2, 2), (2, 3), (3, 2)$ (即ち $q = 4, 8, 9$) に対し、

(1) 素体 $\boldsymbol{F}_p = \boldsymbol{Z}/p\boldsymbol{Z}$ 上 r 次の既約多項式 $f(X) \in \boldsymbol{F}_p[X]$ を、とにかく見付けよ。
(2) $f(X)$ が $\boldsymbol{F}_p$ 上既約であることを、とにかく示せ。
(3) $K := \boldsymbol{F}_p[X]/(f)$ により q 元体 K を構成し、その乗積表を書け。
(4) Frobenius 同型 $\varphi : K \to K; a \mapsto a^p$ の関数表 (a と $\varphi(a)$ との対応表) を作れ。
(5) $\varphi^n = \mathrm{id}_K$ となる最小の正整数 n は何か。

問 13–4. 一般に、体拡大 L/K と、その自己同型群 $\mathrm{Aut}(L/K)$ の部分群 G とに対し、$L^G := \{x \in L | \forall \sigma \in G : \sigma(x) = x\}$ は L/K の中間体を成す。(G による**固定体 (fixed field)** という。)

問 13–5. p 元体 $\boldsymbol{F}_p$ を含む代数閉体 Ω を一つ固定する。任意の正整数 $r \geq 1$ に対し、Ω には位数 $q := p^r$ の部分体 $\boldsymbol{F}_q$ が一意に含まれる。実際、$\boldsymbol{F}_q = \{x \in \Omega | x^q = x\}$ である。

問 13–6. (次問の準備) 位数 n の巡回群を C_n と書く。$n|m$ とするとき、$G := C_n \times C_m$ に対し、$x^n = 1$ となる G の元 $x \in G$ の個数は ?

問 13–7. 体 K の乗法群 $K^\times$ の有限部分群 G は巡回群。(ヒント: 前問及び有限アーベル群の構造定理を用いよ。) 特に、$K = \boldsymbol{F}_q$: 有限体に対し、$\boldsymbol{F}_q^\times$ は巡回群。

問 13–8. 前問により、素数 p に対し、$(\boldsymbol{Z}/p\boldsymbol{Z})^\times$ は巡回群である。その生成元を、法 p に関する**原始根 (primitive root)** という。幾つかの素数 p に対し、原始根を求めよ。

問 13–9. (Fermat の小定理) p を素数とするとき、p と互いに素な整数 a に対し、$a^{p-1} \equiv 1 \pmod{p}$。

問 13–10. p を素数とする。自然数 r に対し、$\boldsymbol{F}_p$ 係数の monic (最高次係数が 1) な r 次多項式全体の集合を M_r、その中で既約なもの全体の集合を N_r とし、$m_r := \#M_r, n_r := \#N_r$ とする。

(1) $m_r = ?$
(2) $n_1 = ?$ monic で可約な 2 次多項式の個数は ? $n_2 = ?$
(3) monic で可約な 3 次多項式の個数は ? $n_3 = ?$
(4) $\displaystyle\sum_{1 \leq d | r} d n_d = p^r$ を示せ。
(5) $\forall r$ に対し、$n_r > 0$ である。即ち、r 次既約多項式が存在する。

問 13–11. K を標数 $p > 0$ の体、$a \in K$ とする。

(1) $f(X) = X^p - a \in K[X]$ は分離的か。f の 1 根を $\alpha \in \overline{K}$ とする時、f の $\overline{K}[X]$ での既約分解は ?
(2) $g(X) = X^p - X - a \in K[X]$ は分離的か。g の 1 根を $\beta \in \overline{K}$ とする時、g の $\overline{K}[X]$ での既約分解は ?
(3) f, g が K 上既約な条件は ? 特に K が有限体の場合はどうなるか。

問 13–12. 次の拡大 $K/\boldsymbol{Q}$ は (有限次分離拡大なので) 単拡大である。生成元の例を挙げ、その $\boldsymbol{Q}$ 上の最小多項式を求めよ。

(1) $K = \boldsymbol{Q}(\sqrt{-1}, \sqrt{-5})$ (2) $K = \boldsymbol{Q}(\sqrt[3]{2}, \omega)$ (但し、$\omega^2 + \omega + 1 = 0$)

問 13–13. $\boldsymbol{F}_p$ 上の 2 変数有理関数体 $L = \boldsymbol{F}_p(t, s)$ とその部分体 $K = \boldsymbol{F}_p(t^p, s^p)$ とを考える。

(1) 体拡大 $L = K(t, s)/K$ の拡大次数 $[L : K] = ?$
(2) 拡大 L/K は単拡大ではない。
(3) 拡大 L/K には中間体が無限個ある。