Exercises in Algebra IIB No.7

1. Show that $\sqrt{5} \notin \mathbb{Q}(\sqrt{2}, \sqrt{7}, \sqrt{11}, \sqrt{13})$.

2. Let $\theta \in \overline{\mathbb{Q}}$ be an algebraic number. Then show that $\mathbb{Q}(\theta)$ and $\mathbb{Q}[\theta]$ are isomorphic. In particular, write $(2 + 2\theta + \theta^2)^{-1}$ in terms of a polynomial of θ when $\theta = \sqrt[3]{2}$.

3. Let K be a field. Find all automorphisms of $K(X)$ over K.

4. Let K be a field. Find all automorphisms of $K(\!(X)\!)$ over K.

5. Determine all monic irreducible polynomials of degree n $(2 \leq n \leq 4)$ in $\mathbb{F}_2[X]$.

6. Check that $X^2 + 2$ and $X^2 + X + 1$ are both irreducible in $\mathbb{F}_5[X]$. Construct concretely an isomorphism between $\mathbb{F}_5[X]/(X^2 + 2)$ and $\mathbb{F}_5[X]/(X^2 + X + 1)$.

7. Let p be a prime and a a non-zero element of $\mathbb{F}_p$. Then show that $X^p - X - a$ is irreducible in $\mathbb{F}_p[X]$.

8. Find a condition of prime numbers p such that $f(X) = X^4 + X^3 + X^2 + X + 1$ can be expressed as a product of different four linear forms in $\mathbb{F}_p[X]$.

9. Show that $\mathrm{GL}(n, \mathbb{F}_p)$ has a cyclic subgroup of order $p^n - 1$.

10. Let $p \geq 7$ be a prime and $\{a_n\}_{n=0}^{\infty}$ the Fibonacci sequence. Let t be the smallest positive integer such that $a_{n+t} \equiv a_n \pmod{p}$ for $\forall n \geq 0$. Then show that $t \mid (p^2 - 1)$.

11. Let q be a power of a prime number and n a positive integer.
    (1) Show that
    $$X^{q^n} - 1 = \prod_i f_i(X) \in \mathbb{F}_q[X],$$
    where the product takes all the monic irreducible polynomials $f_i(X) \in \mathbb{F}_q[X]$ with $\deg f_i \mid n$.
    (2) Let $N(q, n)$ be the number of the monic irreducible polynomials of degree n in $\mathbb{F}_q[X]$. Then show that
    $$N(q, n) = \frac{1}{n} \sum_{d \mid n} \mu\left(\frac{n}{d}\right) q^d,$$
    where $\mu(x)$ is the Möbius function.
    (3) Show that
    $$\sharp\{\theta \in \mathbb{F}_{q^n} \mid \mathbb{F}_q(\theta) = \mathbb{F}_{q^n}\} = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) q^d.$$

12. Let $K = \mathbb{F}_q$ and $L = \mathbb{F}_{q^n}$. Then show the following equalities:

(1) $t_{L/K}(x) = \sum_{i=0}^{n-1} x^{q^i}$.
(2) $N_{L/K}(x) = x^{(q^n-1)/(q-1)}$.
Show moreover that $t_{L/K}$ and $N_{L/K}$ map L surjectively onto K.

13 Let $k = \mathbb{F}_q$, and $a \in k^\times$. Then show that

$$^\sharp\{(x,y) \in k^2 \,|\, x^2 - ay^2 = 1\} = \begin{cases} q-1 & \text{if } \sqrt{a} \in k \\ q+1 & \text{if } \sqrt{a} \notin k. \end{cases}$$