Westlake University
Fundamental Algebra and Analysis I

Exercise sheet 6 - 3 : linear algebra : polynomial and formal power series

You probably think that one knows everything about polynomials.
– Serge Lang

1. Find the quotient and remainder of $f(T)$ dividing $g(T)$.

(1) $f(T) = T^5 + 4T^4 + T^2 + 2T + 3$, $g(T) = T - 2$;

(2) $f(T) = T^n - 1$, $g(T) = T - a$, where a is a scalar.

2. Find the greatest common divisor of $f(T)$ and $g(T)$.

(1) $f(T) = T^5 + T^4 - 5T^3 - 5T^2 + 4T + 4$, $g(T) = T^4 + T^3 - 17T^2 - 21T + 36$;

(2) $f(T) = 3T^4 - 8T^2 - 3$, $g(T) = T^3 - 2T^2 - 3T + 6$.

3. Find a polynomial $P \in \mathbb{R}[T]$ divisible by $T^2 + 1$ such that $P(T) + 1$ is divisible by $T^3 + T^2 + 1$.

4. Suppose $f \in k[T]$, $f(f(T)) = (f(T))^k$, where $k \in \mathbb{N}$. Find all such f.

5. Let a, b be two strictly positive real numbers. Find all positive integer n, such that the polynomial $T^2 - (a^2 + b^2)$ can devise $T^{2n} - (a^n + b^n)^2$ in $\mathbb{R}[T]$.

6. Find the polynomial $f(T)$ with the smallest degree, such that the remainder of $f(T)$ dividing $(T - 1)^2$ is $2T$, and the remainder of $f(T)$ dividing $(T - 2)^2$ is $3T$.

7. Let k be a field. In the k-algebra $k[T]$, we consider the sub-k-algebra $\mathscr{A}$ generated by T^2 and T^3, noted $\mathscr{A} = k[T^2, T^3]$. Prove that $k[T]$ and $\mathscr{A}$ are not isomorphic as k-algebras.

8. Let K and L be two fields. If the rings $K[T]$ and $L[T]$ are isomorphic, prove that K and L are isomorphic as fields.

9. Let k be a field, $P \in k[T]$, and $b, c \in \mathbb{N}$ satisfying $\gcd(b, c) = 1$. Prove that $(P^b - 1)(P^c - 1)$ devises $(P - 1)(P^{bc} - 1)$.

10. Let $m_1, \ldots, m_k \in \mathbb{N}^+$. Prove that the least common multiple of the polynomials $(T^{m_i} - 1)_{1 \leqslant i \leqslant k}$ is $T^d - 1$, where $d = \operatorname{lcm}(m_1, \ldots, m_k)$.

11. Let k be a field, and $r_1, \dots r_k \in \mathbb{N}$, such that $0 \leqslant r_1 < \cdots < r_k \leqslant n-1$, where $n \in \mathbb{N}_{\geqslant 2}$. We give $m_1, \dots, m_k \in \mathbb{N}$, such that $m_i \equiv r_i (\mathrm{mod}\, n)$ for $i = 1, \dots, k$. Prove that the remainder in the Euclidean division of $T^{m_1} + \cdots + T^{m_k}$ by $T^n - 1$ in $k[T]$ is $T^{r_1} + \cdots + T^{r_k}$, and calculate the quotient.

12. Let $q, m \in \mathbb{N}^+$. Find a sufficient and necessary condition such that $1 + T^m + \cdots + T^{qm}$ is divisible by $1 + T + \cdots + T^q$ in $k[T]$, where k is a field.

13. Let $g(X), p(X) \in K[X]$ with $\deg(p) > 0$. Prove that there exist polynomials $\{a_i(X)\}_{i \geqslant 0}$, such that $\deg(a_i) < \deg(p)$,

$$g(X) = a_0(X) + a_1(X)p(X) + \cdots + a_{e-1}(X)p(X)^{e-1},$$

and

$$\frac{g(X)}{p(X)^e} = \frac{a_0(X)}{p(X)^e} + \frac{a_1(X)}{p(X)^{e-1}} + \cdots + \frac{a_{e-1}(X)}{p(X)}.$$

Find an analog of this property over $\mathbb{Z}$.

14. Let k be a field, $f(T) = a_n T^n + \cdots + a_0 \in k[T]$, and $c \in k$. We define $f(c) = a_n c^n + \cdots + a_0 \in k$ is the **value** of $f(T)$ at c. If $f(c) = 0$, then we say c is a **root** of $f(T)$, or $T = c$ is a **root** or **solution** to the equation $f(T) = 0$.

(1) Let $f(T) \in k[T]$, and $c \in k$. Prove that the remainder of $f(T)$ divided by $T - c$ is $f(c)$. In particular, $f(T)$ is divisible by $T - c$ if and only if $f(c) = 0$.

(2) When $\deg(f) = n$, prove that $f(T)$ has at most n roots counting multiplicities.

(3) Let $f(T), g(T) \in k[T]$, $\deg(f), \deg(g) \leqslant n$. Suppose there exist $c_0, \dots, c_n \in k$, such that $f(c_i) = g(c_i)$. $i = 0, \dots, n$. Prove that $f(T) = g(T)$.

(4) Let $f(T) \in k[T]$ satisfying $\deg(f) \leqslant n$, and $a_0, \dots, a_n \in k$ be different. Prove

$$f(T) = \sum_{i=0}^{n} \frac{(T - a_0) \cdots (T - a_{i-1})(T - a_{i+1}) \cdots (T - a_n)}{(a_i - a_0) \cdots (a_i - a_{i-1})(a_i - a_{i+1}) \cdots (a_i - a_n)} f(a_i).$$

This is called **Lagrange interpolation formula**.

15. Let k be a field, and $f(T) \in k[T]$. We denote by $f'(T)$ the derivative of $f(T)$. Let $c \in k$, and prove the following results :

(1) c is a multiple root of $f(T)$ if and only if $f(c) = f'(c) = 0$.

(2) c is a multiple root of $f(T)$ if and only if c is a root of $\gcd(f(T), f'(T))$.

(3) If $\gcd(f(T), f'(T)) = 1$, then $f(T)$ has no multiple root (even in the extension of k).

(4) If $f(T)$ is irreducible over k and $f'(T) \neq 0$, then $f(T)$ has no multiple root (even in the extension of k).

(5) Let $p(T) \in k[T]$ be irreducible. Then $p(T)$ is a multiple factor of $f(T)$ if and only if $p(T)$ is a common factor of $f(T)$ and $f'(T)$.

(6) $f(T)$ has no common factor if and only if $\gcd(f(T), f'(T)) = 1$.

16. Let k be a field, k' is an extension of k. Let $a \in k'$, and we denote

$$J(a) = \{f \in k[T] \mid f(a) = 0\}.$$

Suppose $J(a) \neq \{0\}$.

(1) Prove that there exists the unique polynomial $m(T)$ whose leading coefficient is 1, such that $J(a) = \{h(T)m(T) \mid h(T) \in k[T]\}$.

(2) Prove that the previous $m(T)$ is irreducible.

17. Expand the following rational functions as formal power series.

(1) $\frac{1}{1+T+\cdots+T^{n-1}}$, where $n \in \mathbb{N}_{\geqslant 2}$.

(2) $\frac{1}{(1-aT)^p(1-bT)^q}$, where $a \neq b$, $p, q \in \mathbb{N}^+$.

(3) $\frac{1}{(1-T^p)(1-T^q)}$ with p and q are coprime.

18. For an $n \in \mathbb{N}$, let u_n be the number of permutations $\sigma \in \mathfrak{S}_n$ such that $\sigma^2 = \mathrm{Id}$. We put $u_0 = u_1 = 1$.

(1) Prove that for all $n \in \mathbb{N}_{\geqslant 2}$, we have $u_n = u_{n-1} + (n-1)u_{n-2}$.

(2) We consider the formal power series $S = \sum\limits_{n\geqslant 0} \frac{u_n}{n!} T^n \in \mathbb{C}[\![T]\!]$. Prove that $S' - (1+T)S = 0$, and deduce that $S = \exp\left(T + \frac{T^2}{2}\right)$. Deduce the expression of u_n.