Part V

Modular Polynomials

Polynomials

Definition 5.1.1

Let R be a ring (such as $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/m$, etc.). Then a *polynomial over* R (or, a *polynomial with coefficients in* R) is an expression

$$f(T) = a_d T^d + \cdots + a_1 T + a_0,$$

where T is the variable and the coefficients $a_0, a_1, \cdots, a_d$ belongs to R. The set of polynomials over R is denoted by $R[T]$.

The addition and multiplication of polynomials are defined in the obvious way. (So, using terminology from Algebra, $(R[T], +, 0, \cdot, 1)$ is a ring.)

Example 5.1.2

Try to simplify $(\overline{2}T^2 + T)(\overline{3}T + \overline{2})$ over $\mathbb{Z}/6$.

Example 5.1.2

Try to simplify $(\overline{2}T^2 + T)(\overline{3}T + \overline{2})$ over $\mathbb{Z}/6$.

$$
\begin{aligned}
(\overline{2}T^2 + T)(\overline{3}T + \overline{2}) &= \overline{2}T^2 \cdot \overline{3}T + T \cdot \overline{3}T + \overline{2}T^2 \cdot \overline{2} + T \cdot \overline{2} \\
&= \overline{2} \cdot \overline{3}T^3 + \overline{3}T^2 + \overline{2} \cdot \overline{2}T^2 + \overline{2}T \\
&= \overline{6}T^3 + \overline{3}T^2 + \overline{4}T^2 + \overline{2}T \\
&= \overline{6}T^3 + \overline{3+4}T^2 + \overline{2}T \\
&= T^2 + \overline{2}T.
\end{aligned}
$$

Polynomials over $\mathbb{Z}/m$ can be obtained from those over $\mathbb{Z}$ through the modulo reduction process:

$$\begin{array}{c} a_d T^d + \cdots + a_1 T + a_0 \\ \big\downarrow \; (\mathrm{mod}\ m) \\ \overline{a_d} T^d + \cdots + \overline{a_1} T + \overline{a_0} \end{array}$$

Such a process gives a surjective map respecting the addition, multiplication, and their neutral elements. (Using terminology from Algebra, it is a surjective homomorphism.)

Definition 5.1.3

Two integer polynomials $f(T)$ and $g(T)$ are *congruence modulo* m if for each exponent d, the coefficients of T^d in $f(T)$ and $g(T)$ are congruence modulo m.

This gives an equivalence relation on $\mathbb{Z}[T]$ and each equivalence class is called a *polynomial modulo* m.

Then the reduction map in previous slide identify the quotient set of $\mathbb{Z}[T]$ up to congruence modulo m (i.e. the set of polynomial modulo m) with $\mathbb{Z}/m[T]$. We'll thus not distinguish the two structures.

Polynomials over $\mathbb{Z}/m$ may behave very different from the usual ones (over $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$). However, when p is a prime, polynomials modulo p behave well.

In what follows, we will use the notation $\mathbb{F}_p$ to denote the (ring) structure $\mathbb{Z}/p$ (where p is a prime). The letter $\mathbb{F}$ stands for "*field*", which means a ring in which nonzero = invertible.

Definition 5.1.4

The *degree* of a polynomial $f(T)$ is the largest exponent d, for which the coefficient of T^d is nonzero.

Example 5.1.5

The degree of the integer polynomial $6T^3 + 7T^2 + 2T$ is 3, while the degree of the polynomial $\overline{6}T^3 + \overline{7}T^2 + \overline{2}T$ over $\mathbb{Z}/6$ is 2.

Usually, the degree of the zero polynomial is by convenience -1.

Theorem 5.1.6

Let f, g be two nonzero polynomials over $\mathbb{F}_p$, then we have

$$\deg(fg) = \deg f + \deg g.$$

Theorem 5.1.6

Let f, g be two nonzero polynomials over $\mathbb{F}_p$, then we have

$$\deg(fg) = \deg f + \deg g.$$

Proof. Suppose the leading terms of f and g are $\overline{a}T^{\deg(f)}$ and $\overline{b}T^{\deg(g)}$ respectively. Then we have

$$\begin{aligned} fg &= (\overline{a}T^{\deg(f)} + \text{lower terms})(\overline{b}T^{\deg(g)} + \text{lower terms}) \\ &= \overline{ab}T^{\deg f + \deg g} + \text{lower terms}. \end{aligned}$$

Note that, from $\overline{a} \neq \mathbf{0}$ and $\overline{b} \neq \mathbf{0}$, we have $p \nmid ab$ since p is a prime. Therefore, the degree of fg is $\deg f + \deg g$. $\square$

Theorem 5.1.6

Let f, g be two nonzero polynomials over $\mathbb{F}_p$, then we have

$$\deg(fg) = \deg f + \deg g.$$

N.B. this is not true for $\mathbb{Z}/m$ with m composite.
E.g. over $\mathbb{Z}/6$, we have

$$(\overline{2}T^2 + T)(\overline{3}T + \overline{2}) = T^2 + \overline{2}T.$$

2 + 1 ≠ 2

But the degrees of the factors are 2 and 1.

Definition 5.1.7

We say that a congruence class $\bar{a} \in \mathbb{Z}/m$ is a *root* of the integer polynomial $f(T) \in \mathbb{Z}[T]$, or the integer a is a *root of $f(T)$ modulo m*, if $f(a) \equiv 0 \pmod{m}$.

Definition 5.1.7

We say that a congruence class $\overline{a} \in \mathbb{Z}/m$ is a *root* of the integer polynomial $f(T) \in \mathbb{Z}[T]$, or the integer a is a *root of* $f(T)$ *modulo* m, if $f(a) \equiv 0 \pmod{m}$.

Example 5.1.8

Let's consider 5 and the polynomial $f(T) = 3T^2 + 2T$.

The congruence classes $\overline{0}$ and $\overline{1}$ are roots of f in $\mathbb{F}_5$, while $\overline{2}$, $\overline{3}$, and $\overline{4}$ are not.

Theorem 5.1.9

Consider a linear integer polynomial $f(T) = aT + b$. If $p \nmid a$, then f has a unique root in $\mathbb{F}_p$.

Proof. If $p \nmid a$, then a is invertible modulo p. Hence, by its cancelling property, we get a unique congruence class $-[a]_p^{-1}[b]_p$ being the root of $f(T)$ in $\mathbb{F}_p$. $\square$

Theorem 5.1.9

Consider a linear integer polynomial $f(T) = aT + b$. If $p \nmid a$, then f has a unique root in $\mathbb{F}_p$.

N.B. this is not true for $\mathbb{Z}/m$ with m composite.
E.g. in $\mathbb{Z}/6$, the linear polynomial $3T + 1$ has no roots, while $3T + 3$ has three roots: $\overline{1}$, $\overline{3}$, and $\overline{5}$.