MATH1050 Basic results on polynomials 'beyond school mathematics'

1. **Polynomials with real coefficients, according to school maths.**

   Let $a_0, a_1, a_2, \cdots, a_n$ be real numbers. Consider the formal sum $a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$.

   Suppose $a_n \neq 0$. Then this formal sum is called a **degree-n polynomial with real coefficients and with indeterminate** *x. The number n is called the* **degree** *of this polynomial.*

   We agree to write $a_j = 0$ for each $j > n$, and write this polynomial as $a_0 + a_1x + a_2x^2 + \cdots$, when it is convenient to do so.

   For each $j \in \mathbb{N}$, the expression a_jx^j is called the **degree-j term** *of this polynomial, and the number a_j the* **j-th coefficient** *of this polynomial.*

   a_nx^n is also called the **leading term** *of this polynomial, and the number a_n the* **leading coefficient**. *If $a_n = 1$, then this polynomial is said to be* **monic**.

   a_0 is also called the **constant term** *of this polynomial.*

   Terminologies and conventions.

   (a) **Zero polynomial.**

   The formal sum $0 + 0 \cdot x + 0 \cdot x^2 + \cdots + 0 \cdot x^k + \cdots$ is called the **zero polynomial**. We denote it by 0, and declare its degree to be $-\infty$.

   (b) **Non-constant polynomials.**

   Each polynomial of degree at least 1 is called a non-constant polynomial. The degree-0 polynomials together with the zero polynomial are referred to as constant polynomials.

   (c) **Functional notations and substitutions of numbers.**

   For convenience, we agree to use the functional notation (such as $u(x)$, $v(x)$, $w(x)$) for denoting such polynomials.

   Suppose $u(x)$ is the polynomial with real coefficients given by $u(x) = a_0 + a_1x + a_2x^2 + \cdots$. Then the real number $a_0 + a_1\alpha + a_2\alpha^2 + \cdots$ obtained by substituting $x = \alpha$ into $u(x)$ is denoted by $u(\alpha)$.

   (d) **Notation for degrees of polynomials.**

   Let $u(x)$ be a polynomial with real coefficients. We denote its degree by $\deg(u(x))$.

   Remark. We write $\deg(0) = -\infty$. (Here 0 refers to the zero polynomial.)

   (e) **Equality for polynomials.**

   Suppose $u(x), v(x)$ are polynomials with real coefficients given by $u(x) = a_0 + a_1x + a_2x^2 + \cdots$, $v(x) = b_0 + b_1x + b_2x^2 + \cdots$. We agree to declare that $u(x)$ is the same as $v(x)$ exactly when $a_j = b_j$ for each j. In this situation we write $u(x) = v(x)$ as polynomials.

   A consequence of $u(x) = v(x)$ as polynomials is that $u(\alpha) = v(\alpha)$ for each real number α.

   (f) **Arithmetic operations for polynomials.**

   Suppose $u(x) = a_0 + a_1x + a_2x^2 + \cdots$, $v(x) = b_0 + b_1x + b_2x^2 + \cdots$ as polynomials, with the k-th coefficients of $u(x), v(x)$ being the real numbers a_k, b_k respectively for each $k \in \mathbb{N}$.

   i. **Addition.** We define $u(x) + v(x)$ by

   $$u(x) + v(x) = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \cdots + (a_k + b_k)x^k + \cdots .$$

   So, for each $k \in \mathbb{N}$, the k-th coefficient of the sum $u(x) + v(x)$ is given by $a_k + b_k$.

   ii. **Scalar multiplication.**
   For each real number C, we define $Cu(x)$ by

   $$Cu(x) = (Ca_0) + (Ca_1)x + (Ca_2)x^2 + \cdots + (Ca_k)x^k + \cdots .$$

   So, for each $k \in \mathbb{N}$, the k-th coefficient of the scalar multiple $Cu(x)$ is given by Ca_k.

   iii. **Subtraction.**
   We define $u(x) - v(x)$ by

   $$u(x) - v(x) = u(x) + (-1 \cdot v(x)) = (a_0 - b_0) + (a_1 - b_1)x + (a_2 - b_2)x^2 + \cdots + (a_k - b_k)x^k + \cdots .$$

   So, for each $k \in \mathbb{N}$, the k-th coefficient of the difference $u(x) - v(x)$ is given by $a_k - b_k$.

iv. **Multiplication.**
We define $u(x)v(x)$ by

$$u(x)v(x) = (a_0b_0) + (a_1b_0 + a_0b_1)x + (a_2b_0 + a_1b_1 + a_0b_2)x^2 + \cdots + \left(\sum_{j=0}^{k} a_jb_{k-j}\right)x^k + \cdots .$$

So, for each $k \in \mathbb{N}$, the k-th coefficient of the product $u(x)v(x)$ is given by $\sum_{j=0}^{k} a_jb_{k-j}$.

Remark. Note that each of the equalities above is an equality for polynomials; they should be understood in the sense that the respective coefficients in the polynomials of the two sides of the equality symbol '=' agree with each other. (In school maths textbooks, the words *identical as polynomials*, *polynomial identities* are used instead of *equal as polynomial*, *polynomial equalities* here.)

Much of what you have learnt about arithmetic for polynomials in school maths can be summarized as Theorem (0).

Theorem (0).

Denote by $\mathbb{R}[x]$ the set of all polynomials with real coefficients and with indeterminate x.

(a) *$\mathbb{R}[x]$ forms a commutative ring with unity, with addition and multiplication provided by polynomial addition and polynomial multiplication respectively.*

(b) *$\mathbb{R}[x]$ forms a vector space over $\mathbb{R}$, with vector addition and scalar multiplication provided by polynomial addition and scalar multiplication for polynomials respectively.*

Proof of Theorem (0). Exercise.

2. **Observation.**

Every definition stated above concerned with polynomials with real coefficients, together with Theorem (0), relies upon the validity of the rules of arithmetic for $+, -, \times, \div$ in the real number system.

For this reason, everything stated above concerned with polynomial with real coefficients can be carried over when the field $\mathbb{R}$ is replaced by a general field $\mathbb{F}$, the phrase 'real number' is replaced by the phrase 'field element (of $\mathbb{F}$)', and $+, -, \times, \div$ in $\mathbb{R}$ are replaced by the corresponding operations in $\mathbb{F}$.

3. *From this point on, we will work with the same field $\mathbb{F}$.*

Theorem (1).

Denote by $\mathbb{F}[x]$ the set of all polynomials with coefficients in $\mathbb{F}$ and with indeterminate x.

(a) *$\mathbb{F}[x]$ forms a commutative ring with unity, with addition and multiplication provided by polynomial addition and polynomial multiplication respectively. The addition identity is the zero polynomial, and the multiplicative identity is the constant polynomial 1.*

(b) *$\mathbb{F}[x]$ forms a vector space over $\mathbb{F}$, with vector addition and scalar multiplication provided by polynomial addition and scalar multiplication for polynomials respectively.*

4. **Theorem (2).**

Let $u(x), v(x)$ be polynomials with coefficients in $\mathbb{F}$ and with indeterminate x. Suppose neither of $u(x), v(x)$ is the zero polynomial. Then $\deg(u(x)v(x)) = \deg(u(x)) + \deg(v(x))$.

Remark.

- By 'extending' the 'laws of arithmetic' for integers to incorporate '$-\infty$' (the 'minus infinity') and the equalities

  '$(-\infty) + m = -\infty$', '$m + (-\infty) = -\infty$' whenever m is 'finite',

  '$(-\infty) + (-\infty) = -\infty$,

  we may extend the conclusion '$\deg(u(x)v(x)) = \deg(u(x)) + \deg(v(x))$' in Theorem (1) to the situation in which $u(x) = 0$ or $v(x) = 0$.

We expect from intuition that multiplying a non-constant polynomial with whatever polynomial which is 'non-zero' results in a non-constant polynomial. This is in fact an immediate consequence of Theorem (2):

Corollary to Theorem (2).

Let $u(x), v(x)$ be polynomials with coefficients in $\mathbb{F}$.

Suppose $u(x)v(x)$ is a non-zero constant polynomial. Then each of $u(x), v(x)$ is a non-zero constant polynomial.

5. **Proof of Theorem (2).**

   Let $u(x), v(x)$ be polynomial with coefficients in $\mathbb{F}$ and with indeterminate x. Suppose neither of $u(x), v(x)$ is the zero polynomial.

   For each $j \in \mathbb{N}$, denote the j-th coefficient of $u(x), v(x), u(x)v(x)$ by a_j, b_j, c_j respectively.

   Denote the degrees of $u(x), v(x)$ by m, n respectively.

   By definition, we have $a_m \neq 0$ and $b_n \neq 0$. Also, $a_k = 0$ whenever $k > m$, and $b_\ell = 0$ whenever $\ell > n$.

   By definition, for each $r \in \mathbb{N}$, we have $c_r = \sum_{k=0}^{r} a_k b_{r-k}$. [Ask: Is it true that $c_{m+n} \neq 0$ and $c_s > 0$ whenever $s > m + n$?]

   - We have

$$c_{m+n} = \sum_{k=0}^{m+n} a_k b_{m+n-k} = \underbrace{\sum_{k=0}^{m-1} a_k b_{m+n-k}}_{b_{m+n-k} = 0 \text{ for each } k} + a_m b_n + \underbrace{\sum_{k=m+1}^{m+n} a_k b_{m+n-k}}_{a_k = 0 \text{ for each } k} = a_m b_n \neq 0.$$

   - Suppose $s > m + n$. Then

$$c_s = \sum_{k=0}^{s} a_k b_{s-k} = \underbrace{\sum_{k=0}^{m} a_k b_{s-k}}_{b_{s-k} = 0 \text{ for each } k} + \underbrace{\sum_{k=m+1}^{s} a_k b_{s-k}}_{a_k = 0 \text{ for each } k} = 0.$$

   It follows that $\deg(u(x)v(x)) = m + n = \deg(u(x)) + \deg(v(x))$.

6. **Theorem (3). (Absence of 'zero-divisors'.)**

   Let $u(x), v(x)$ be polynomials with coefficients in $\mathbb{F}$.

   Suppose $u(x)v(x)$ is the zero polynomial. Then at least one of $u(x), v(x)$ is the zero polynomial.

   Proof. Exercise. (Modify the argument for Theorem (2).)

   Remarks.

   - Hence the product of a pair of polynomials, neither being the zero polynomial, is not the zero polynomial.

   Theorem (3) looks 'intuitively' but is non-trivial. Combined with Theorem (1), it gives:

   Corollary to Theorem (3).

   $\mathbb{F}[x]$ forms an integral domain with addition and multiplication given by polynomial addision and polynomial multiplication respectively.

7. **Definition. (Divisibility for polynomials.)**

   Let $u(x), v(x)$ be polynomials with coefficients in $\mathbb{F}$. The polynomial $u(x)$ is said to be **divisible** *by the polynomial $v(x)$ if there exists some $k(x)$ with coefficients in $\mathbb{F}$ such that $u(x) = k(x)v(x)$ as polynomials.*

   Remarks.

   - According to definition, the zero polynomial is divisible by the zero polynomial. However, no polynomial except the zero polynomial is divisible by the zero polynomial.
   - Each polynomial with coefficients in $\mathbb{F}$ is divisible by every non-zero constant polynomial with coefficients in $\mathbb{F}$, and by every non-zero-scalar multiple of itself.

- Each linear polynomial with coefficient in $\mathbb{F}$ is divisible by no linear polynomials other than the non-zero-scalar multiple of itself.

Examples.

(a) i. As a polynomial with real coefficients, x^2+1 is divisible by each of

$$1, \quad x^2+1$$

but no other monic polynomials with real coefficients.

ii. As a polynomial with complex coefficients, x^2+1 is divisible by each of

$$1, \quad x-i, \quad x+i, \quad x^2+1$$

but no other monic polynomials with complex coefficients.

(b) i. As a polynomial with real coefficients, x^2-2 is divisible by each of

$$1, \quad x-\sqrt{2}, \quad x+\sqrt{2}, \quad x^2-2$$

but no other monic polynomials with real coefficients.

ii. As a polynomial with complex coefficients, x^2-2 is divisible by each of

$$1, \quad x-\sqrt{2}, \quad x+\sqrt{2}, \quad x^2-2$$

but no other monic polynomials with complex coefficients.

(c) i. As a polynomial with real coefficients, x^3+x^2+x+1 is divisible by each of

$$1, \quad x-1, \quad x^2+1, \quad x^3+x^2+x+1$$

but no other monic polynomials with real coefficients.

ii. As a polynomial with complex coefficients, x^3+x^2+x+1 is divisible by each of

$$1, \quad x-1, \quad x-i, \quad x+i, \quad x^2+1, \quad x^2+(-1-i)x+i, \quad x^2+(-1+i)x-i, \quad x^3+x^2+x+1$$

but no other monic polynomials with complex coefficients.

(d) i. As a polynomial with real coefficients, x^3-2 is divisible by each of

$$1, \quad x-\sqrt[3]{2}, \quad x^2+\sqrt[3]{2}\cdot x+(\sqrt[3]{2})^2, \quad x^3-2$$

but no other monic polynomials with real coefficients.

ii. As a polynomial with complex coefficients, x^3-2 is divisible by each of

$$1, \qquad x-\sqrt[3]{2}, \qquad x-\sqrt[3]{2}\cdot\omega, \qquad x-\sqrt[3]{2}\cdot\omega^2,$$

$$x^2+\sqrt[3]{2}\cdot x+(\sqrt[3]{2})^2, \qquad x^2+\sqrt[3]{2}\cdot\omega^2 x+(\sqrt[3]{2})^2\omega, \qquad x^2+\sqrt[3]{2}\cdot\omega x+(\sqrt[3]{2})^2\omega^2, \qquad x^3-2$$

but no other monic polynomials with complex coefficients. Here ω is the number $\dfrac{-1}{2}+\dfrac{\sqrt{3}}{2}i$. (It is a cubic root of unity.)

Further examples.

(a) Refer to Theorem (9) in the Handout *Basic results on complex numbers 'beyond school mathematics'*. Suppose $u(x)$ is a quadratic polynomial with complex coefficients. Then the polynomial $u(x)$ has a pair of (not necessarily distinct) roots, say, α, β, in $\mathbb{C}$. It is divisible by the linear polynomials $x-\alpha$, $x-\beta$ but no other monic linear polynomials with complex coefficients. In fact, given that $\gamma \in \mathbb{C}\backslash\{\alpha,\beta\}$, we have $u(\gamma)\neq 0$, and we can deduce the equality $u(x)=a(x-\gamma)(x-\delta)+u(\gamma)$ as polynomials for some $a,\delta\in\mathbb{C}$ (after brute-force calculation). It follows that $u(x)$ is not divisible by $x-\gamma$. (Why?)

(b) Refer to Theorem (1) in the Handout *Quadratic polynomials*.

Suppose $u(x)$ is a quadratic polynomial with real coefficients, given by $u(x) = c + bx + ax^2$. The discriminant of $u(x)$ is the number $b^2 - 4ac$, denoted by Δ.

i. Suppose $\Delta \geq 0$. Then $u(x)$ has a pair of (not necessarily distinct) real roots, say, α, β. Modifying the discussion above for quadratic polynomials with complex coefficients, we will come to the conclusion that $u(x)$ is divisible by the linear polynomials $x - \alpha$, $x - \beta$ but no other monic linear polynomials with real coefficients.

ii. Suppose $\Delta < 0$. Then $u(x)$ is divisible by no linear polynomials with real coefficients. (Why?)

8. **Theorem (4). (A special case of Division Algorithm for polynomials.)**

Let $u(x)$ be a polynomial with coefficients in $\mathbb{F}$. Suppose α is a number in $\mathbb{F}$. Then there exists some unique polynomial $v(x)$ with coefficients in $\mathbb{F}$ such that $u(x) = (x - \alpha)v(x) + u(\alpha)$ as polynomials.

Proof of Theorem (4). The result follows from Lemma (4E) and Lemma (4U).

Remarks.

- Here $u(\alpha)$ stands for the number in $\mathbb{F}$ obtained by substituting '$x = \alpha$' into the polynomial $u(x)$. It is (deliberately) confused with the constant polynomial whose only term is the number $u(\alpha)$.
- Within the context of the statement of Theorem (4), we refer to the polynomial $v(x)$ and the constant polynomial $u(\alpha)$ as the **quotient** and the **remainder** in the division of the polynomial $u(x)$ by the linear polynomial $x - \alpha$.

The Remainder Theorem and the Factor Theorem that you learnt in school maths are immediate consequences of Theorem (4).

Corollary (1) to Theorem (4). (Remainder Theorem.)

Let $u(x)$ be a polynomial with coefficients in $\mathbb{F}$. Let α be a number in $\mathbb{F}$. There exists some unique polynomial $v(x)$ with coefficients in $\mathbb{F}$ and some unique number r in $\mathbb{F}$, namely $r = u(\alpha)$, such that $u(x) = (x - \alpha)v(x) + r$ as polynomials.

Corollary (2) to Theorem (4). (Factor Theorem.)

Let $u(x)$ be a polynomial with coefficients in $\mathbb{F}$. Let α be a number in $\mathbb{F}$.

$u(x)$ is divisible by $x - \alpha$ iff $u(\alpha) = 0$.

Proof of the Factor Theorem.

Let $u(x)$ be a polynomial with coefficients in $\mathbb{F}$. Let α be a number in $\mathbb{F}$. By Theorem (4), there exists some unique polynomial $v(x)$ with coefficients in $\mathbb{F}$ such that $u(x) = (x - \alpha)v(x) + u(\alpha)$ as polynomials.

- Suppose $u(\alpha) = 0$. Then $u(x) = (x - \alpha)v(x)$ as polynomials. By the definition of divisibility, $u(x)$ is divisible by $x - \alpha$.
- Suppose $u(x)$ is divisible by $x - \alpha$. Then there exists some polynomial $k(x)$ with coefficients in $\mathbb{F}$ such that $u(x) = (x - \alpha)k(x)$ as polynomials. Now, substituting $x = \alpha$, we obtain $u(\alpha) = 0$.

9. **Lemma (4U). (Uniqueness part of Theorem (4).)**

Let $u(x)$ be a polynomial with coefficients in $\mathbb{F}$. Suppose α is a number in $\mathbb{F}$. Let $v(x), w(x)$ be polynomials with coefficients in $\mathbb{F}$. Suppose $u(x) = (x - \alpha)v(x) + u(\alpha)$ and $u(x) = (x - \alpha)w(x) + u(\alpha)$ as polynomials. Then $v(x) = w(x)$ as polynomials.

Proof of Lemma (4U).

Let $u(x)$ be a polynomial with coefficients in $\mathbb{F}$. Suppose α is a number in $\mathbb{F}$. Let $v(x), w(x)$ be polynomials with coefficients in $\mathbb{F}$. Suppose $u(x) = (x - \alpha)v(x) + u(\alpha)$ and $u(x) = (x - \alpha)w(x) + u(\alpha)$ as polynomials.

Then $(x - \alpha)v(x) = u(x) - u(\alpha) = (x - \alpha)w(x)$ as polynomials.

Therefore $(x - \alpha)(v(x) - w(x)) = 0$ as polynomials.

By Theorem (3), at least one of $x - \alpha$, $v(x) - w(x)$ is the zero polynomial.

Note that $x - \alpha$ is not the zero polynomial. Then $v(x) - w(x) = 0$ as polynomials. Therefore $v(x) = w(x)$ as polynomials.

10. **Lemma (4E). (Existence part of Theorem (4).)**

Let $u(x)$ be a polynomial with coefficients in $\mathbb{F}$. Suppose α is a number in $\mathbb{F}$. Then there exists some polynomial $v(x)$ with coefficients in $\mathbb{F}$ such that $u(x) = (x-\alpha)v(x) + u(\alpha)$ as polynomials.

Proof of Lemma (4E).

Let $u(x)$ be a polynomial with coefficients in $\mathbb{F}$. Suppose α is a number in $\mathbb{F}$.

There exist some $a_0, a_1, a_2, \cdots, a_n \in \mathbb{F}$ such that $u(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ as polynomials.

Note that $u(\alpha) = a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n$.

Define the polynomial $g_1(x)$ with coefficients in $\mathbb{F}$ by $g_1(x) = 1$. For each $r = 2, 3, \cdots, n$, define the polynomial $g_j(x)$ with coefficients in $\mathbb{F}$ by

$$g_r(x) = \alpha^{r-1} + \alpha^{r-2}x + \alpha^{r-3}x^2 + \cdots + \alpha x^{r-2} + x^{r-1}.$$

We have

$$u(x) - u(\alpha) = \sum_{j=1}^{n} a_j(x^j - \alpha^j) = \sum_{j=1}^{n} a_j(x-\alpha)g_j(x) = (x-\alpha)\sum_{j=1}^{n} a_j g_j(x) \quad \text{as polynomials.}$$

Define the polynomial $v(x)$ with coefficients in $\mathbb{F}$ by $v(x) = \sum_{j=1}^{n} a_j g_j(x)$. We have $u(x) - u(\alpha) = (x-\alpha)v(x)$ as polynomials. Then $u(x) = (x-\alpha)v(x) + u(\alpha)$ as polynomials.

Remark.

- We can give an alternative argument for Lemma (4E) with the help of mathematical induction. The beginning of the argument is given here:

  Let α be a number in $\mathbb{F}$. Suppose $u(x)$ is a constant polynomial. Then $u(x) = u(\alpha) = (x-\alpha)\cdot 0 + u(\alpha)$ as polynomials.
  Denote by $P(n)$ the proposition below:
  - *Suppose $u(x)$ is a polynomial of degree n with coefficients in $\mathbb{F}$. Then there exists some polynomial $v(x)$ of degree $n-1$ with coefficients in $\mathbb{F}$ such that $u(x) = (x-\alpha)v(x) + u(\alpha)$ as polynomials.*

  Now proceed to verify $P(1)$ and the statement '*For any $k \in \mathbb{N}\backslash\{0\}$, if $P(k)$ is true then $P(k+1)$ is true*'. Et cetera.

11. **Theorem (5). (Properties of divisibility.)**

The statements below hold:

(a) *Suppose $u(x)$ is a polynomial with coefficients in $\mathbb{F}$. Then $u(x)$ is divisible by $u(x)$.*

(b) *Let $u(x), v(x)$ be polynomials with coefficients in $\mathbb{F}$. Suppose $u(x)$ is divisible by $v(x)$ and $v(x)$ is divisible by $u(x)$. Then there exists some $c \in \mathbb{F}\backslash\{0\}$ such that $u(x) = cv(x)$ as polynomials.*

(c) *Let $u(x), v(x), w(x)$ be polynomials with coefficients in $\mathbb{F}$. Suppose $u(x)$ is divisible by $v(x)$ and $v(x)$ is divisible by $w(x)$. Then $u(x)$ is divisible by $v(x)$.*

Proof of Theorem (5). Exercise. (Imitate the argument for the analogous results for integers.)

12. **Theorem (6). (Further properties of divisibility.)**

Let $t(x)$ be a polynomial with coefficients in $\mathbb{F}$. The statements below hold:

(a) *Let $u(x), v(x)$ be polynomials with coefficients in $\mathbb{F}$. Suppose $u(x)$ is divisible by $t(x)$ and $v(x)$ is divisible by $t(x)$. Then $u(x) + v(x)$ is divisible by $t(x)$.*

(b) *Let $u(x), v(x)$ be polynomials with coefficients in $\mathbb{F}$. Suppose $u(x)$ is divisible by $t(x)$ or $v(x)$ is divisible by $t(x)$. Then $u(x)v(x)$ is divisible by $t(x)$.*

Proof of Theorem (6). Exercise. (Imitate the argument for the analogous results for integers.)

We denote by $\mathbb{F}[x]$ the set of all polynomials with coefficients in $\mathbb{F}$ and with indeterminate x.

13. **Theorem (7). (Division Algorithm for polynomials.)**

Let $u(x), v(x) \in \mathbb{F}[x]$. Suppose $v(x)$ is not the zero polynomial. Then there exist some unique $q(x), r(x) \in \mathbb{F}[x]$ such that $u(x) = q(x)v(x) + r(x)$ as polynomials and ($\deg(r(x)) < \deg(v(x))$ or $r(x) = 0$).

Remarks.

(a) In the statement of Theorem (7), the polynomials $q(x)$, $r(x)$ are called the **quotient** and **remainder** in the division of $u(x)$ by $v(x)$.

(b) Theorem (4) is a special case of Theorem (7).

(c) As in the proof of the Division Algorithm for natural numbers (Theorem (DAN)), the proof of Theorem (7) is made up of an argument for its 'existence part' and a separate argument for its 'uniqueness part'. The argument for the 'existence part' relies on the Well-Ordering Principle for integers (or equivalently, Principle of Mathematical Induction); it resembles the argument for the 'existence part' of Theorem (DAN). The argument for the 'uniqueness part' resembles that for the 'uniqueness part' of Theorem (DAN).

Proof of Theorem (7). The result follows from Lemma (7E) and Lemma (7U). The argument for Lemma (7E) relies on the Well-Ordering Principle for integers (or equivalently, Principle of Mathematical Induction).

14. **Lemma (7E). (Existence part of Theorem (7).)**

Let $u(x), v(x) \in \mathbb{F}[x]$. Suppose $v(x)$ is not the zero polynomial. Then there exist some $q(x), r(x) \in \mathbb{F}[x]$ such that $u(x) = q(x)v(x) + r(x)$ as polynomials and ($\deg(r(x)) < \deg(v(x))$ or $r(x) = 0$).

Proof of Lemma (7E).

Let $u(x), v(x) \in \mathbb{F}[x]$. Suppose $v(x)$ is not the zero polynomial.

Define $S = \{t(x) \in \mathbb{F}[x] : t(x) = u(x) - s(x)v(x) \text{ for some } s(x) \in \mathbb{F}[x]\}$.

- (Case 1). Suppose $0 \in S$. Then there exists some $q(x) \in \mathbb{F}[x]$ such that $u(x) = q(x)v(x) + 0$ as polynomials.
- (Case 2.) Suppose $0 \notin S$. Then every element of S has a degree, which is at least 0.
  Define $S' = \{\deg(t(x)) \mid t(x) \in S\}$. By definition, $S' \subset \mathbb{N}$.
  Since $u(x) \in S$, we have $S \neq \emptyset$. Then $S' \neq \emptyset$.
  According to the Well-Ordering Principles for Integers, the set S' has a least element, say, m.
  By the definition of S', there exists some $r(x) \in S$ such that $\deg(r(x)) = m$.
  By definition, $r(x) \in \mathbb{F}[x]$ and $r(x) \neq 0$.
  Also by definition there exists some $q(x) \in \mathbb{F}[x]$ such that $r(x) = u(x) - q(x)v(x)$ as polynomials. Then for the same $q(x), r(x) \in \mathbb{F}[x]$, we have $u(x) = q(x)v(x) + r(x)$ as polynomials.
  We verify that $\deg(r(x)) < \deg(v(x))$, with a proof-by-contradiction argument:

  Suppose it were true that $\deg(r(x)) \geq \deg(v(x))$.
  [Under this assumption, we are going to construct some polynomial $\tilde{r}(x)$ with coefficients in $\mathbb{F}$ which satisfies $\tilde{r}(x) \in S$ and $\deg(\tilde{r}(x)) < \deg(r(x))$. This existence of such a polynomial is a contradiciton.]
  Write the leading term of $r(x)$ as ax^m. By definition, $a \in \mathbb{F}\backslash\{0\}$.
  Write the leading term of $v(x)$ as bx^n. By definition, $b \in \mathbb{F}\backslash\{0\}$.
  By assumption, we would have $m = \deg(r(x)) \geq \deg(v(x)) = n$.
  Then $b^{-1}ax^{m-n}$ is a polynomial of degree $m - n$.
  Now $b^{-1}ax^{m-n}v(x)$ is a polynomial of degree m and leading term ax^m.
  Define $\tilde{r}(x) = r(x) - b^{-1}ax^{m-n}v(x)$. By definition, $\tilde{r}(x) \in \mathbb{F}[x]$.
  We have

$$\tilde{r}(x) = r(x) - b^{-1}ax^{m-n}v(x) = u(x) - q(x)v(x) - b^{-1}ax^{m-n}v(x) = u(x) - (q(x) + b^{-1}ax^{m-n})v(x)$$

  as polynomials.
  Then $\tilde{r}(x) \in S$.
  Now, by definition, $\deg(\tilde{r}(x)) \in S'$. Then $\deg(\tilde{r}(x)) \geq m$.
  By construction, the leading term of $\tilde{r}(x)$ is of degree less than m. Contradiction arises.

15. **Lemma (7U) . (Uniqueness part of Theorem (7).)**

Let $u(x), v(x) \in \mathbb{F}[x]$. Suppose $v(x)$ is not the zero polynomial. Let $q(x), r(x), p(x), s(x) \in \mathbb{F}[x]$. Suppose $u(x) = q(x)v(x) + r(x)$ as polynomials and ($\deg(r(x)) < \deg(v(x))$ or $r(x) = 0$) and $u(x) = p(x)v(x) + s(x)$ as polynomials and ($\deg(s(x)) < \deg(v(x))$ or $s(x) = 0$). Then $q(x) = p(x)$ and $r(x) = s(x)$ as polynomials.

Proof of Lemma (7U).

Let $u(x), v(x) \in \mathbb{F}[x]$. Suppose $v(x)$ is not the zero polynomial. Let $q(x), r(x), p(x), s(x) \in \mathbb{F}[x]$. Suppose $u(x) = q(x)v(x) + r(x)$ as polynomials and ($\deg(r(x)) < \deg(v(x))$ or $r(x) = 0$) and $u(x) = p(x)v(x) + s(x)$ as polynomials and ($\deg(s(x)) < \deg(v(x))$ or $s(x) = 0$).

We have $(q(x) - p(x))v(x) = s(x) - r(x)$ as polynomials.

Suppose it were true that $s(x) - r(x) \neq 0$. Then $q(x) - p(x) \neq 0$.

By Theorem (2), we have $\deg(q(x) - p(x)) + \deg(v(x)) = \deg(s(x) - r(x))$.

Then $\deg(s(x) - r(x)) \geq \deg(v(x))$.

Note that $r(x) = 0$ or $r(x) \neq 0$.

- (Case 1.) Suppose $r(x) = 0$. Then $s(x) \neq 0$. Therefore $\deg(s(x)) < \deg(v(x)) \leq \deg(s(x) - r(x)) = \deg(s(x))$. Contradiction arises.
- (Case 2.) Suppose $r(x) \neq 0$. Then $\deg(r(x)) < \deg(v(x))$.

  Now $\deg(s(x) - r(x)) \geq \deg(v(x)) > \deg(r(x))$. Since $s(x) = (s(x) - r(x)) + r(x)$ as polynomials, $s(x)$ is a non-zero polynomial with degree $\deg(s(x) - r(x))$. But $\deg(s(x)) < \deg(v(x))$ by assumption. Contradiction arises.

In any case we have a contradiction. Hence in the first place, it is false that $s(x) - r(x) \neq 0$.

Therefore we have $s(x) = r(x)$ as polynomials. Hence $p(x) = q(x)$ as polynomials also.

16. **Corollary to Theorem (7).**

Let $u(x), v(x) \in \mathbb{F}[x]$. Suppose $v(x)$ is not the zero polynomial. Then $u(x)$ is divisible by $v(x)$ iff the remainder is the zero polynomial in the division of $u(x)$ by $v(x)$.

Remark. This result provides the connection between the definition of divisibility for polynomials and Division Algorithm for polynomials.

17. **Beyond Division Algorithm for polynomials.**

With the notions of divisibility and degree for polynomials over fields, we can define *common divisors* and *greatest common divisor* for polynomial over fields.

We can formulate the *Euclidean Algorithm* for polynomial over fields with the help of Division Algorithm for polynomials over fields, and prove it with the help of the Well-Ordering Principle for Integers. We may systematically obtain the greatest common divisor for any pair of distinct non-zero polynomials over fields. There are also *Bezout's Identity* and *Euclid's Lemma* for polynomial over fields, analogous to results of the same names for integers.

Analogous to prime numbers are *irreducible polynomials*. Analogous to the Fundamental Theorem of Arithmetic is the *Existence and Uniqueness Theorem for unique factorizations of polynomials in terms of irreducible polynomials*.

As hinted by the statement of Theorem (7) and the argument for it, the notion of degrees of polynomials is going to play a crucial role in all the above: it provides some kind of 'measurement', in terms of natural numbers, for comparing the 'sizes' of polynomials. It is the analogue for the notion of absolute value for the corresponding results for integers.

The full story will unfold in your *algebraic structures* course.

18. **Appendix. Polynomials over a field, formally defined.**

We now proceed to build a theoretical foundation for the notion of polynomials over the field $\mathbb{F}$, which support all the results stated above.

Definition. (Terminating sequences.)

Let $\{a_j\}_{j=0}^{\infty}$ be an infinite sequence in $\mathbb{F}$. Suppose there exists some $N \in \mathbb{N}$ such that $a_r = 0$ whenever $r \geq N$. Then we call $\{a_j\}_{j=0}^{\infty}$ a terminating sequence in $\mathbb{F}$.

Definition. (Polynomials and polynomial functions over a field.)

A polynomial with coefficients in $\mathbb{F}$ *is a terminating sequence in* $\mathbb{F}$.

Suppose such a terminating sequence is given by $\{a_j\}_{j=0}^{\infty}$. *Then we agree that the polynomial concerned may be presented as the formal expression*

$$a_0 + a_1x + a_2x^2 + \cdots + a_kx^k + \cdots .$$

The symbol x *is called the indeterminate in (this presentation of) the polynomial.*

For each $j \in \mathbb{N}$, *the expression* a_jx^j *is called the* **degree-**j **term** *of this polynomial, and the number* a_j *is called the* j**-th coefficient** *of this polynomial. The* 0*-th coefficient* a_0 *is also called the constant term of this polynomial.*

- *Suppose* $a_k \neq 0$ *for some* $k \in \mathbb{N}$. *Then the least element in the set* $\{j \in \mathbb{N} : a_r = 0 \text{ for any } r > j\}$ *(whose existence is guaranteed by the Well-ordering Principle for Integers) is called the* **degree** *of this polynomial. For the moment, denote this number by* n.

  By definition $a_n \neq 0$, *and* $a_r = 0$ *whenever* $r > n$. *In light of this, we (usually) agree to write the polynomial as*

  $$a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1} + a_nx^n.$$

  The degree-n *term* a_nx^n *is called the leading term of this polynomial, and* a_n *the leading coefficient of this polynomial.*

- *Suppose* $a_j = 0$ *for each* $j \in \mathbb{N}$. *Then the polynomial is presented as*

  $$0 + 0 \cdot x + 0 \cdot x^2 + \cdots + 0 \cdot x^k + \cdots$$

  In this situation, we call the polynomial the zero polynomial. We may write this polynomial as 0, *and declare its degree to be negative infinity.*

It is 'natural' (as in school maths) to deliberately (and purposefully) confuse the polynomial

$$a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1} + a_nx^n$$

with the function with domain $\mathbb{F}$ *and range* $\mathbb{F}$ *defined by* $x \longmapsto a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ *for any* $x \in \mathbb{F}$. *This function from* $\mathbb{F}$ *to* $\mathbb{F}$ *is called the* **polynomial function** *associated to the polynomial* $a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1} + a_nx^n$.

When we label such a function by, say, u, *we will also immediately 'borrow' the 'functional notation'* $u(x)$ *back as a label for the polynomial* $a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$, *and write*

$$u(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \quad \text{as polynomials.}$$

We now denote the degree of this polynomial by $\deg(u(x))$.

The set of all polynomials with coefficients in $\mathbb{F}$ *and with indeterminate* x *is denoted by* $\mathbb{F}[x]$.

Definition. (Equality for polynomials.)

Suppose $u(x), v(x)$ *are two polynomials with coefficients in* $\mathbb{F}$ *and with indeterminate* x, *given by* $u(x) = a_0 + a_1x + a_2x^2 + \cdots + a_kx^k + \cdots$, $v(x) = b_0 + b_1x + b_2x^2 + \cdots + b_kx^k + \cdots$ *respectively.*

We say that $u(x)$ *is equal to* $v(x)$ *as polynomials, and write* $u(x) = v(x)$ *as polynomials, if* $a_j = b_j$ *for any* $j \in \mathbb{N}$.

Definition. (Sums and products for infinite sequences in $\mathbb{F}$**.)**

Let $\{a_j\}_{j=0}^{\infty}$, $\{b_j\}_{j=0}^{\infty}$ be infinite sequences in $\mathbb{F}$.

(a) The **sum** of $\{a_j\}_{j=0}^{\infty}$, $\{b_j\}_{j=0}^{\infty}$ is defined to be the infinite sequence $\{a_j + b_j\}_{j=0}^{\infty}$ in $\mathbb{F}$.

(b) The **product** of $\{a_j\}_{j=0}^{\infty}$, $\{b_j\}_{j=0}^{\infty}$ is defined to be the infinite sequence $\left\{\sum_{r=0}^{j} a_jb_{r-j}\right\}_{j=0}^{\infty}$ in $\mathbb{F}$.

Lemma (A1).

Suppose $\{a_j\}_{j=0}^{\infty}$, $\{b_j\}_{j=0}^{\infty}$ *are terminating sequences in* $\mathbb{F}$.

Then the sum and the product of $\{a_j\}_{j=0}^{\infty}$, $\{b_j\}_{j=0}^{\infty}$ *are terminating sequences in* $\mathbb{F}$.

Proof of Lemma (A1). Exercise. (Apply the Well-ordering Principle for integers.)

Corollary (A2). (Sums and products for polynomials.)

Suppose $u(x), v(x)$ *are two polynomials with coefficients in* $\mathbb{F}$ *and with indeterminate* x, *given by* $u(x) = a_0 + a_1x + a_2x^2 + \cdots + a_kx^k + \cdots$, $v(x) = b_0 + b_1x + b_2x^2 + \cdots + b_kx^k + \cdots$ *respectively. The statements below hold:*

(a) *The sum of* $u(x), v(x)$, *which is defined to be*

$$(a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \cdots + (a_k + b_k)x^k + \cdots,$$

is well-defined as a polynomial with coefficients in $\mathbb{F}$.

(b) *The product of* $u(x), v(x)$, *which is defined to be*

$$a_0b_0 + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + \cdots + \left(\sum_{r=0}^{k} a_rb_{k-r}\right) x^k + \cdots,$$

is well-defined as a polynomial with coefficients in $\mathbb{F}$.

Proof of Lemma (A2). This is an immediate consequence of Lemma (A1).

Remark. The point of this result is to *make sense* of the sum and the product of two polynomials *as polynomials*, which (though intuitively obvious) needs be formulated and verified carefully. We can similarly make sense of the difference between two polynomials as a polynomial. The scalar product for polynomials is just a special case of the product of two polynomials.