MATH 2040 Linear Algebra II
Supplementary Notes by Martin Li

Polynomials [1]

The notion of polynomial must already be familiar to you. In this note, we will give some properties of polynomial that would be useful in this course. There are in fact many different ways to view polynomials as an object. A common approach is to think of a polynomial simply as an expression of the form

$$p(z) = a_0 + a_1 z + a_2 z^2 \cdots + a_n z^n,$$

where z is just a "*dummy variable*" which does not carry any algebraic or geometric meaning. However, from our experience (e.g. in calculus), it is also useful to consider polynomials as a special kind of functions. We will take this as our definition. Recall that $\mathbb{F}$ denotes either $\mathbb{R}$ or $\mathbb{C}$ in this note [2].

Definition 1. *A function $p : \mathbb{F} \to \mathbb{F}$ is called a **polynomial** with coefficients in $\mathbb{F}$ if there exists $a_0, a_1, \cdots, a_m \in \mathbb{F}$ such that*

$$p(z) = a_0 + a_1 z + a_2 z^2 \cdots + a_m z^m \qquad \textit{for all } z \in \mathbb{F}.$$

It is easy to see that the coefficients $a_0, \cdots, a_m$ are uniquely determined by the function $p : \mathbb{F} \to \mathbb{F}$ as follows. Suppose there exist another set of coefficients $b_0, \cdots, b_n$, possibly $n \neq m$, such that

$$p(z) = b_0 + b_1 z + b_2 z^2 \cdots + b_n z^n \qquad \text{for all } z \in \mathbb{F}.$$

Without loss of generality, let us assume $n \leq m$ and define $b_{n+1} = \cdots = b_m = 0$. Subtracting the two expressions above, we obtain a polynomial which is equal to the zero function. The uniqueness of coefficients then follows from the lemma below.

Lemma 2. *Suppose $a_0 + a_1 z + a_2 z^2 + \cdots + a_m z^m = 0$ for all $z \in \mathbb{F}$ (where $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$). Then, $a_0 = a_1 = \cdots = a_m = 0$.*

Proof. We will prove the lemma by contradiction. Suppose $a_m \neq 0$. Then we can define a positive number $z > 0$ where

$$z := \frac{|a_0| + |a_1| + \cdots + |a_{m-1}|}{|a_m|} + 1.$$

Since $z > 1$, by the triangle inequality and the definition of z,

$$|a_0 + a_1 z + \cdots + a_{m-1} z^{m-1}| \leq (|a_0| + \cdots |a_{m-1}|) z^{m-1} < |a_m| z^m.$$

Therefore, $a_0 + a_1 z + a_2 z^2 + \cdots + a_m z^m \neq 0$ for this particular z defined above. This gives a contradiction. $\square$

The lemma above not only implies that it is equivalent to think of a polynomial as a formal expression and a function, but it also implies the the degree of a polynomial is well-defined.

[1] last revised on September 5, 2017

[2] In fact, many of our discussions make sense for $\mathbb{F}$ to be any *field* for example $\mathbb{F} = \mathbb{Z}_2$ (or even a *ring*).

Definition 3. *A polynomial $p : \mathbb{F} \to \mathbb{F}$ is said to have* **degree** *m (where $m \geq 0$) if there exist $a_0, \cdots, a_m \in \mathbb{F}$ with $a_m \neq 0$ such that*

$$p(z) = a_0 + a_1 z + a_2 z^2 \cdots + a_m z^m \qquad \text{for all } z \in \mathbb{F}.$$

If a polynomial is identically zero, then the degree is defined to be $-\infty$. We use the symbol $\deg(p)$ to denote the degree of a polynomial p.

Proposition 4. *For any polynomial p, q with coefficients in $\mathbb{F}$, we have*

$$\deg(pq) = \deg(p) + \deg(q).$$

Proof. Exercise. (Note that it is true even when one (or both) of p and q is identically zero.) □

We now summarize a few basic properties of polynomials that would come in handy in this course. We will skip all the proofs for the sake of simplicity.

Proposition 5 (Division algorithm)**.** *Let p and s be two polynomials with coefficients in $\mathbb{F}$ where s is not identically zero, then there exist polynomials r, q with coefficients in $\mathbb{F}$ such that $\deg(r) < \deg(s)$ and*

$$p = sq + r.$$

The solution to a polynomial equation $p(z) = 0$ plays an important role in the study of polynomials. A number $\lambda \in \mathbb{F}$ is said to be a **zero** (or a **root**) of p if $p(\lambda) = 0$.

Lemma 6. *A number $\lambda \in \mathbb{F}$ is a root of a polynomial p if and only if there exists some polynomial q with coefficients in $\mathbb{F}$ such that $p(z) = (z - \lambda)q(z)$ for every $z \in \mathbb{F}$.*

The lemma above immediately implies the following:

Theorem 7. *A polynomial with coefficients in $\mathbb{F}$ of degree m has at most m distinct roots in $\mathbb{F}$.*

Theorem 8 (Fundamental Theorem of Algebra)**.** *Every non-constant polynomial with complex coefficients has a zero.*

Corollary 9. *Every non-constant polynomial $p(z)$ with complex coefficients has a unique factorization (up to re-ordering the factors) of the form*

$$p(z) = c(z - \lambda_1) \cdots (z - \lambda_m)$$

where $c, \lambda_1, \cdots, \lambda_m \in \mathbb{C}$. Here, $\lambda_1, \cdots, \lambda_m$ are the (possibly not distinct) roots of p.

Lemma 10. *Let p be a polynomial with real coefficients. If we treat p as a complex polynomial, then $\lambda \in \mathbb{C}$ is a root of p if and only if $\overline{\lambda} \in \mathbb{C}$ is a root of p.*

Corollary 11. *Every non-constant polynomial $p(z)$ with real coefficients has a unique factorization (up to re-ordering the factors) of the form*

$$p(x) = c(x - \lambda_1) \cdots (x - \lambda_m)(x^2 + b_1 x + c_1) \cdots (x^2 + b_M x + c_M),$$

where $c, \lambda_1, \cdots, \lambda_m, b_1, \cdots, b_M, c_1, \cdots, c_M \in \mathbb{R}$ with $b_j^2 < 4c_j$ for each j.