Univariate Polynomials (Linear Algebra 2)

PACS numbers:

I. POLYNOMIALS OVER A FIELD

A. Basics and factorization over $\mathbb{C}$ and $\mathbb{R}$

Let $(\mathbb{F}, \cdot, +)$ be a field. Most of this course we will work over infinite fields (indeed we will restrict mostly to $\mathbb{F} = \mathbb{R}, \mathbb{C}, \mathbb{Q}$). When working over infinite fields we can identify a polynomial with the polynomial function i.e. both contains the same information, which leads to the definition[1]

Definition. A **polynomial with coefficients in** $\mathbb{F}$ is a function $p : \mathbb{F} \to \mathbb{F}$ of the form

$$p(x) = \sum_{i=0}^{n} a_i x^i \qquad a_i \in \mathbb{F} \ \text{ for all } \ i \tag{1}$$

we denote the set of all polynomial with coefficients in $\mathbb{F}$ as $\mathbb{F}[x]$ and we define the degree ($\deg(p)$)of p as $n \in \mathbb{Z}_{\geq 0} \cup \{-\infty\}$ where n is the highest integer such that $a_n \neq 0$ and $\deg(p = 0) = -\infty$. We call then a polynomial monic if $a_n = 1$. Polynomials are entirely determined by its coefficients and so two polynomials being equal, means their coefficients are equal. We can define the following operations on polynomials:

- **Addition**: $(p + g)(x) = \sum_{i=0}^{\max(\deg(p), \deg(g))} (a_i + b_i) x^i$
- **Product**: $(p \cdot g)(x) = \sum_{i=0}^{\deg(p)+\deg(g)} \left(\sum_{j=0}^{i} a_i b_{j-i} \right) x^i$

one can the show that $(\mathbb{F}[x], \cdot, +)$ forms a commutative ring.

Theorem(division theorem). Let $p, d \in \mathbb{F}[x]$ with $d \neq 0$, then there exist a unique pair $q, r \in \mathbb{F}[x]$ such that

- $p = qd + r$
- $\deg(r) < \deg(d)$

Theorem (remainder theorem). Let $p \in \mathbb{F}[x]$ and $c \in \mathbb{F}$, then the remainder of dividing p by $(x - c)$ is $p(c)$.

Proposition. Let $p, g \in \mathbb{F}[x]$ then

- If $c_1, \ldots, c_k$ are distinct roots of p, then $\prod_{i=1}^{k} (x - c_i) | p$.
- Let $n \in \mathbb{Z}_{\geq 1}$, then if $\deg(p) = n$, p has at most n distinct roots.
- Let $n \in \mathbb{Z}_{\geq 1}$, and $\deg(p) \leq n$ and $\deg(g) \leq n$. If $p(x_i) = g(x_i)$ for $i = 1, \ldots, n + 1$ with $x_1, \ldots, x_{n+1}$ all distinct, then $p = g$.

Theorem(fundamental theorem of algebra). Let $p \in \mathbb{C}[x]$ with $\deg(p) \geq 1$, then p as at least one complex root.

Important consequences of this theorem are the following:

---

[1] The identification between a polynomial and a polynomial function is not 1-1 when working, for example, over finite fields. However, we will not go into details about finite fields, so identifying polynomial with its polynomial function is fine for us. See S.Lang *Undergraduate Algebra*, Chapter IV for a detailed explanation of the difference between these, if you are interested.

Theorem(factorization of a polynomial over $\mathbb{C}$). Let $p \in \mathbb{C}[x]$ with $\deg(p) \geq 1$, then p as a unique factorization (up to ordering of the factors) of the form:

$$p(x) = c\prod_{i=1}^{n}(x-\lambda_i) \qquad c, \lambda_1, \ldots, \lambda_n \in \mathbb{C} \tag{2}$$

Theorem(factorization of a polynomial over $\mathbb{R}$). Let $p \in \mathbb{R}[x]$ with $\deg(p) \geq 1$, then p as a unique factorization (up to ordering of the factors) of the form:

$$p(x) = c\left(\prod_{i=1}^{n}(x-\lambda_i)\right)\prod_{j=1}^{m}(x^2+b_jx+c_j) \qquad c, \lambda_1, \ldots, \lambda_n, b_1, \ldots, b_m, c_1, \ldots, c_m \in \mathbb{R} \tag{3}$$

with $b_j^2 < 4c_j$ for all j.

B. Irreducibility and gcd

We can extend various properties of integers to commutative rings with no zero divisors such as $(\mathbb{F}[x], \cdot, +)$.

Definition. The **greatest common divisor** (gcd) between two nonzero polynomials $p, g \in \mathbb{F}[x]$ is a polynomial $h = gcd(p, g)$ satisfying:

- $h|p$ and $h|g$.
- For all $f \in \mathbb{F}[x]$ that divides p and g then $f|h$.

Note that, in this form, $h = gcd(p, g)$ is only defined up to multiplication by a nonzero constant. One can alternatively add an extra requirement to h, we can require that is monic, then is unique.

Definition. $p \in \mathbb{F}[x]$ is said to be **irreducible over** $\mathbb{F}$ if it cannot be written as $f = hg$ with $h, g \in \mathbb{F}[x]$ nonconstant polynomials (i.e., the degree of h and g must be at least 1).

Note how important is to specify over which field we define irreducibility over. For example $x^2 + 1$ is irreducible over $\mathbb{R}$ but reducible over $\mathbb{C}$.

Theorem(factorization of a polynomial over any field $\mathbb{F}$). Let $p \in \mathbb{F}[x]$ with $\deg(p) \geq 1$, then p as a unique factorization (up to ordering of the factors) of the form:

$$p(x) = c\prod_{i=1}^{m}p_i \tag{4}$$

where p_i, $i = 1, \ldots, m$ are monic polynomials, irreducibles over $\mathbb{F}$.

This theorem is valid over any field $\mathbb{F}$, finite or infinite. When all nonconstant polynomials in $\mathbb{F}[x]$ have at least one root in $\mathbb{F}$,, we say that $\mathbb{F}$ is algebraically closed. We have only studied one algebraically closed field, namely $\mathbb{C}$. We can also write (4) as $p(x) = c\prod_{i=1}^{k}p_i^{m_i}$ with $p_1, \ldots, p_k$ distinct, then m_i is called the multiplicity of p_i in p. So, if $\mathbb{F}$ is algebraically closed, then all irreducibles are of degree 1 i.e. $p_i = x - \lambda_i$ and then m_i is called the multiplicity of the root λ_i (if m_i, is said to be a simple root and a multiple root otherwise).

C. Polynomials over $\mathbb{Q}$ or $\mathbb{Z}$

$\mathbb{Q}$ is a field, but note that $\mathbb{Z}$ is not, yet is an integral domain. We call a polynomial $p \in \mathbb{Z}[x]$ **primitive** if all its coefficients are relatively prime (for example, if such p is monic, then is primitive). Note then, any $f \in \mathbb{Q}[x]$ can be multiplied by a constant $c \in \mathbb{Q}$ such that $cf \in \mathbb{Z}[x]$ and cf is primitive.

Lemma(Gauss). If $p, g \in \mathbb{Z}[x]$ are primitive, then so is pg.

Theorem(Gauss). Let $p \in \mathbb{Z}[x]$ be a primitive, nonconstant polynomial. Then, if p is reducible over $\mathbb{Q}$, then is reducible over $\mathbb{Z}$.

Corollary. Let $p \in \mathbb{Z}[x]$ be a primitive, nonconstant polynomial. Then, if p is irreducible over $\mathbb{Z}$, then is irreducible over $\mathbb{Q}$.

Note in this theorem and its corollary, the importance of specifying over which field we are stating irreducibility.

Theorem(Eisenstein's criteron). Consider a nonconstant polynomial $f \in \mathbb{Z}[x]$ of degree n,

$$f(x) = \sum_{i=1}^{n} a_i x^i \tag{5}$$

and suppose there exist a prime p such that

$$p \mid a_i \;\; \text{for} \;\; i = 0, \ldots, n-1 \qquad p \nmid a_n \qquad p^2 \nmid a_0 \tag{6}$$

then f is irreducible over $\mathbb{Q}$.

Definition. $a \in \mathbb{C}$ is called an **algebraic number** if a is the root of a polynomial with rational coefficients i.e. $\exists\, p \in \mathbb{Q}[x]$ such that $p(a) = 0$.

Proposition. For every algebraic number a, there exist a unique monic polynomial $p \in \mathbb{Q}[x]$ of lowest degree such that $p(a) = 0$. p is called the minimal polynomial of a. Moreover every polynomial $g \in \mathbb{Q}[x]$ satisfying $g(a) = 0$, is divisible by p and p is irreducible over $\mathbb{Q}$.