Polynomials

April 28, 2017

1 Polynomials over $\mathbb{F}$

Let $\mathbb{F}$ be a field.

Definition 1.1: *A **polynomial** over $\mathbb{F}$ in the variable X is given by a (formal) expression of the form $P(X) = a_n X^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_0$ where $n \in \mathbb{N}$ and $a_j \in \mathbb{F}$ for all j with $0 \leq j \leq n$. The a_j are called the **coefficients** of P. We sometimes define $a_j = 0$ for all $j \geq n$.*

The set of all polynomials over $\mathbb{F}$ in the variable X is denoted by $\mathbb{F}[X]$.

Definition 1.2: *Let P, Q defined by $P(X) = a_n X^n + \ldots + a_0$ and $Q(X) = b_m X^m + \ldots + b_0$, and $\lambda \in \mathbb{F}$ be a scalar. We define the **sum** of P and Q and the product of P by λ as follows*

$$(P+Q)(X) = \sum_{j=0}^{n} (a_j + b_j) X^j$$
$$(\lambda P)(X) = \lambda a_n X^n + \ldots + \lambda a_0$$

This gives $\mathbb{F}[X]$ a structure of vector space over $\mathbb{F}$. It has infinite dimension (a basis is $1, X, X^2, \ldots$). Its zero vector is the **zero polynomial**: the polynomial with all coefficients 0.

But we can add some more structure by defining a product

Definition 1.3: *Let P, Q be given by $P(X) = a_n X^n + \ldots + a_0$ and $Q(X) = b_m X^m + \ldots + b_0$. The **product** of P with Q is*

$$(PQ)(X) = \sum_{k=0}^{n+m} \sum_{i+j=k} a_i b_j X^k$$

Some properties of this product of polynomials (for all $P, Q, R \in \mathbb{F}[X]$, $\lambda \in \mathbb{F}$)

- Associativity of multiplication: $(PQ)R = P(QR)$.
- Commutativity of multiplication: $PQ = QP$.
- Distributivity: $P(Q+R) = PQ + PR$ and $(P+Q)R = PR + QR$.
- Compatibility with scalars: $\lambda(PQ) = (\lambda P)Q = P(\lambda Q)$.

Warning: not every element admits an inverse under multiplication. More on this later.

Definition 1.4: *The highest j such that $a_j \neq 0$ is called the **degree** of P. By convention the zero polynomial is assumed to have degree $-\infty$. A polynomial with degree 0 or $-\infty$ is called a **constant polynomial**.*

*The coefficient $a_{\deg P}$ is called the **leading coefficient** of P, and $a_{\deg P} X^{\deg P}$ is the **leading term** of P. If the leading coefficient is 1, we say that P is **monic**.*

The following lemma describes how degrees behave under sum and product.

Lemma 1.5: *Let P, Q be polynomials. Then*

$$\deg(P+Q) \leq \max\{\deg P, \deg Q\}$$
$$\deg(PQ) = \deg P + \deg Q$$

where the convention is that for any $n \in \{-\infty\} \cup \mathbb{N}$ we agree that $\max\{-\infty, n\} = n$, and $n + (-\infty) = (-\infty) + n = -\infty$.

Proof. Exercise □

In general, we do not have equality in the first line: consider $P(X) = X^2 + X + 1$ and $Q(X) = -X^2$ for example.

Remark 1.6: *If $P(X) = a_n X^n + \ldots + a_0$, and $Q(X) = b_m X^m + \ldots + b_0$, then $\deg(P+Q) < \max\{\deg P, \deg Q\}$ iff $n = m$ and $a_n = -b_m$.*

2 Division of polynomials

In $\mathbb{Z}$ we say that d divides p if there exists $q \in \mathbb{Z}$ such that $p = dq$. We define a similar notion for polynomials.

Definition 2.1: *Let $P, D \in \mathbb{F}[X]$. We say D **divides** P, and write $D \mid P$, if there exists $R \in \mathbb{F}[X]$ such that $P = RD$. We also say that D is a **factor**, or a **divisor** of P; and that P is a **multiple** of D.*

In $\mathbb{Z}$, if d does not divide p, we can do the division of p by d with a remainder $r < |d|$. Ex: 37 divided by 7 "equals" 5 with a remainder of 2, that is, $37 = 5 \times 7 + 2$. In $\mathbb{F}[X]$, we can do a similar operation:

Proposition 2.2: *Let $D, P \in \mathbb{F}[X]$ with $D \neq 0$. There exist unique polynomials $Q, R \in F[X]$ such that $P = QD + R$ and $\deg R < \deg D$.*

This operation is called "Euclidean division".

Proof. (Uniqueness) Suppose $P = QD + R = Q'D + R'$ - then $(Q - Q')D = R' - R$. The right hand side has degree at most $\deg D - 1$, while the left hand side has degree $\deg(Q - Q') + \deg D$, the only possibility for equality is that they are both $-\infty$. Thus we must have $Q = Q'$ and $R = R'$.

(Existence) We define by induction a sequence of pairs Q_n, R_n such that $P = Q_n D + R_n$ and $\deg R_{n+1} < \deg R_n$. After finitely many step this will stop, and we will have $\deg R_m < \deg D$.

To initialize we set $Q_1 = 0$ and $R_1 = P$. We have $P = Q_1 D + R_1$. Suppose we have defined Q_n, R_n with the required properties, and that $\deg R_n \geq \deg D$.

Write $R_n(X) = a_k X^k + \ldots + a_0$ for some $a_k \neq 0$, and $D(X) = d_l X^l + \ldots + d_0$ with $d_l \neq 0$, and $l \leq k$. We define $Q_{n+1} = Q_n + \frac{a_k}{d_l} X^{k-l}$, and $R_{n+1} = P - Q_{n+1} D = R_n - \frac{a_k}{d_l} X^{k-l} D$. We have $Q_{n+1} D + R_{n+1} = Q_n D + R_n = P$. Moreover, R_n and $\frac{a_k}{d_l} X^{k-l} D$ have the same leading term so $\deg R_{n+1} < \deg R_n$.

We can continue in this way until we get Q_m, R_m with $\deg R_m < \deg D$. □

In practice?

Example 2.3: Division of $4X^3 - 2X^2 + 1$ by $X^2 + X + 1$.

$$\begin{array}{rrrr|l}
4X^3 & -2X^2 & & +1 & X^2 \;\; +X \;\; +1 \\
\cline{5-5}
-(4X^3 & +4X^2 & +4X) & & 4X \;\; -6 \\
\cline{1-3}
 & -6X^2 & -4X & +1 & \\
 & -(-6X^2 & -6X & -6) & \\
\cline{2-4}
 & & 2X & +7 &
\end{array}$$

The quotient of the division is $Q(X) = 4X - 6$, while the remainder is $2X + 7$.
You can check that $4X^3 - 2X^2 + 1 = (X^2 + X + 1)(4X - 6) + (2X + 7)$

3 Roots

Each polynomial $P \in \mathbb{F}[X]$ gives us a polynomial function $\mathbb{F} \to \mathbb{F}$ defined by $b \mapsto P(b) = a_n b^n + a_{n-1} b^{n-1} + \ldots + a_1 b + a_0$.

Definition 3.1: *We say that a scalar $a \in \mathbb{F}$ is a **root** of the polynomial P if $P(a) = 0$.*

Note that if Q divides P, any root of Q is a root of P. Indeed, then $P = QR$, so if a satisfies $Q(a) = 0$ then $P(a) = Q(a)R(a) = 0$.

Proposition 3.2: *a is a root of P iff $(X - a)$ divides P*

Proof. Suppose $(X - a)$ divides P: since a is a root of $X - a$, then a is a root of P.

Suppose a is a root of P, that is, $P(a) = 0$. We divide P by $X - a$ to get $P = (X - a)Q + R$ with $\deg R < 1$ - hence R is a constant $r \in \mathbb{F}$. Thus $P(a) = (a - a)Q(a) + R(a) = r$, hence $r = 0$ and $X - a$ divides P. □

Proposition 3.3: *A polynomial of degree $n \geq 0$ has at most n roots.*

Proof. By induction on the degree of P. If $\deg P = 0$, then P is a nonzero constant polynomial, thus it has no roots.

Suppose that any polynomial of degree $< n$ has at most $n - 1$ roots. Let $P \in \mathbb{F}[X]$ of degree n. If P has no roots in $\mathbb{F}$, we are done. If a is a root of P, we can write $P = (X - a)Q$, with $\deg Q = n - 1$.

If $b \in \mathbb{F}$ and $b \neq a$, we have $P(b) = (b - a)Q(b) = 0$, so $P(b) = 0$ iff $Q(b) = 0$. Thus the roots of P are exactly the roots of Q together with a.

But by induction hypothesis, Q has at most $n - 1$ roots, therefore, P has at most n roots. □

The following is sometimes called the fundamental theorem of algebra:

Theorem 3.4: *Any non constant polynomial over $\mathbb{C}$ has a root.*

Corollary 3.5: *If P is a polynomial of degree n over $\mathbb{C}$, then there exist $c_1, \ldots, c_n \in \mathbb{C}$, and $b \in \mathbb{C}$ such that*

$$P(X) = b(X - c_1) \ldots (X - c_n)$$

The c_i's are exactly the roots of P.

Note that the c_i's are not necessarily distinct. The proof is by induction on n.