# UIC Mtht 435 Class notes

## Polynomials

A polynomial $f(X)$ with coefficients in an integral domain $R$ is a finite sum

$$f(X) = \sum_{i=1}^{m} a_i X^i.$$

The symbol $X$ is called a variable, but more formally we may define $f$ to be a sequence of coefficients

$$f = \{a_0, a_1, \ldots, a_m, 0, 0, \ldots\}$$

which has only finitely many nonzero terms $a_i \in R$. The sum and product of polynomials may be defined in terms of such sequences. The polynomial $X$ corresponds to the sequence $\{0, 1, 0, 0, \ldots\}$. The set of polynomials with coefficients in $R$ is a commutative ring $R[X]$. For the $f \in R[X]$ defined above and for $c \in R$, we define the evaluation of $f$ on $c$ to be

$$f(c) = \sum_{i=1}^{m} a_i c^i \in R.$$

We say $g(X)$ divides $f(X)$, written $g(X)|f(X)$, if there is a polynomial $Q$ such that $f(X) = q(X)g(X)$.

If $a_i = 0$ for $i < m$ and $a_m \neq 0$, we say $a_m$ is the leading coefficient, $a_m X^m$ is the leading term, and $m$ is the *degree* of $f$, $\deg f = m$. It is convenient to define the degree of the zero polynomial by $\deg 0 = -\infty$. Then

$$\deg(fg) = \deg f + \deg g \quad \text{and} \quad \deg(f+g) \leq \max\{\deg f, \deg g\}.$$

The formula for $\deg(fg)$ holds because $R$ has no zero divisors. A polynomial is called *monic* if its leading coefficient is 1.

Division Theorem. If $f, g \in R[X]$ and $g$ is monic, then there are unique polynomials $q$ and $r$ such that

$$f(X) = q(X)g(X) + r(X), \quad \text{where} \quad \deg r < \deg g.$$

Proof. Let $\deg f = m$ and $\deg g = n$. Since $g$ is monic, $n \geq 1$.

If $m < n$, set $q(X) = 0$ and $r(X) = f(X)$.

For the case $m \geq n$ we use induction on $m$. Since $0 < n$, the result is proved for $m = 0$. Assume the result has been proved for $\deg f \leq m - 1$.

Recall the long division process; let $m \geq n$ and

$$f(X) = a_m X^m + \text{ lower order terms }, \quad g(X) = X^n + \text{ lower order terms }.$$

The initial step in dividing $g$ into $f$ is

$$\begin{array}{rl} & a_m X^{m-n} \\ \cline{2-2} X^n + \text{ lower order terms } \big) & a_m X^m + \text{ lower order terms} \\ & a_m X^m + \text{ lower order terms} \\ \cline{2-2} & 0 \qquad + \text{ lower order terms}\,. \end{array}$$

Hence $q(X) = a_m X^{m-n} + \text{ lower order terms}\,.$

Since $f(X) - a_m X^{m-n} g(X)$ has degree at most $m-1$, by the inductive hypothesis, there exist $q_1(X)$ and $r_1(X)$ such that

$$f(X) - a_m X^{m-n} g(X) = q_1(X) g(X) + r_1(X) \quad \text{with} \quad \deg r_1 < \deg g$$

and therefore

$$f(X) = \big(a_m X^{m-n} + q_1(X)\big) g(X) + r_1(X).$$

Setting $q(X) = a_m X^{m-n} + q_1(X)$ and $r(X) = r_1(X)$ gives the existence result.

For uniqueness, suppose that also

$$f(X) = \tilde{q}(X) g(X) + \tilde{r}(X), \quad \text{where} \quad \deg r < \deg g.$$

Then $g(q - \tilde{q}) = \tilde{r} - r$ and $\deg(\tilde{r} - r) < \deg g$, hence $\deg g + \deg(q - \tilde{q}) < \deg g$. Therefore $\deg(q - \tilde{q}) < 0$ so $q = \tilde{q}$ and hence $r = \tilde{r}$.

If $F$ is a field and $f \in F[X]$ is not identically zero, then $x \in F$ is a *root* of $f$ if $f(x) = 0$.

Corollary. Let $F$ be a field, $f \in F[X]$, and $x \in F$. Then $x$ is a root of $f$ if and only if $X - x$ divides $f(X)$.

Proof. If $X - x$ divides $f(X)$, then $f(X) = q(X)(X - x)$ and $f(x) = q(x)(x - x) = 0$. In general, by the division theorem $f(X) = q(X)(X - x) + r(X)$ where $\deg r \leq \deg(X - x) = 1$. Therefore $r(X) = r_0$, a constant. If $x$ is a root of $f$ then $r_0 = 0$ and $X - x$ divides $f(X)$

If $(X - x)^k | f(X)$ but $(X - x)^{k+1} \not| f(X)$, then $x$ is called a root of *multiplicity* $k$.

## Algebraic numbers and field extensions

Definition. Let $F \subset K$ be fields. The field $K$ is called an *extension* of $F$. If $x \in K$, then $x$ is *algebraic* over $F$ if there is a nonzero polynomial $p \in F[X]$ with $p(x) = 0$. An element $x \in K$ which is not algebraic is said to be *transcendental.* If every element of $K$ is algebraic over $F$, $K$ is said to be an *algebraic extension* of $F$.

Theorem 2. If $K$ is a finite extension of $F$, $[K : F] = n$, then $K$ is an algebraic extension. Each element $x \in K$ is a root of some polynomial of degree $\leq n$.

Proof. The elements $1, x, x^2, \ldots, x^n$ are linearly dependent over $F$ (since there are more than $n$ of them). Hence there is a dependence relation $\sum_{i=1}^n a_i x^i = 0_K$ where not all the $a_i = 0_F$. Thus $x$ is a root of the nonzero polynomial $p(X) = \sum_{i=1}^n a_i X^i \in F[X]$. This polynomial has degree less than or equal to $n$.

Given $x \in K$ algebraic over $F$, let $p \in F[X]$ be a polynomial of minimal degree such that $x$ is a root of $p$. Then $\deg p \geq 0$ if $x \neq 0$ and $\deg p = 1$ if and only if $0 \neq x \in F$.

A polynomial is called *irreducible* if it is not the product of two polynomials of lower degree. A polynomial $p$ with root $x$ of minimal degree is irreducible in $F[X]$ because if $p$ factored, say $p(X) = g(X)h(X)$, then $g(x)h(x) = 0$ and hence one of these lower degree polynomials would have $x$ as a root. Multiplying $p(X)$ by the inverse in $F$ of its leading coefficient, we get a monic polynomial of the same degree.

If $p$ and $f$ are two monic polynomials of the same degree in $F[X]$, both with root $x$, then $p(X) - f(X)$ is a polynomial of lower degree with root $x$. Therefore there is a unique monic polynomial with root $x$ of minimal degree called *the minimal* polynomial of $x$ over $F$. The *degree of $x$ over $F$* is the degree of this minimal polynomial.

For a fixed $x \in K$, the set $F[x] = \{g(x) : g \in F[X]\} \subset K$ is a commutative ring, $F \subset F[x] \subset K$, and $F[x]$ is a vector space over $F$. The main result we will need is:

THEOREM. Let $F \subset K$ be fields and $a \in K$. The following are equivalent:

(1) $x$ is algebraic of degree $n$ over $F$,

(2) $F[x]$ is an $n$-dimensional vector space over $F$ with basis $1, x, x^2, \ldots, x^{n-1}$,

(3) $F[x]$ is a subfield of $K$ and the index $[F[x] : F] = n$.

PROOF. We show (1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (1). Actually, the proofs give only inequalities on the dimensions, but we fix that at the end.

First assume (1) and let $f$ be the minimal polynomial of $x$. Then

$$x^n = -a_0 - a_1 x - \cdots - a_{n-1} x^{n-1},$$

so $x^n \in L = L(1, x, \ldots, x^{n-1})$. If $x^n, \ldots, x^{n+k} \in L$, then

$$x^{n+k+1} = -a_0 x^{k+1} - a_1 x^{k+2} - \cdots - a_{n-1} x^{n+k} \in L.$$

Hence, by induction, $x^\ell \in L$ for all $\ell \geq 0$. Thus for any $g \in F[X]$, $g(x) \in L$, hence $F[x] = L$. Therefore $1, x, \ldots, x^{n-1}$ is a spanning set for $F[x]$ and $\dim_F F[x] = m \leq n$.

Second assume $\dim_F F[x] = m < \infty$. $F[x]$ is a commutative ring. To prove it is a field we must show every nonzero element $u \in F[x]$ has a multiplicative inverse. Define a map $\phi : F[x] \longrightarrow F[x]$ by $\phi(v) = uv$; the product is in the ring $F[x] \subset K$. This map is a linear map of vector spaces over $F$ since

$$\phi(v + w) = u(v + w) = uv + uw = \phi(v) + \phi(w),$$
$$\phi(cv) = u(cv) = c(uv) = c\phi(v) \text{ for } c \in F.$$

Now $u, v \in K$ and $u \neq 0$ so if $uv = 0$ then $v = 0$. Thus $\ker \phi = \{v \in F[a] : uv = 0\} = \{0\}$ and $\dim \ker \phi = 0$. Therefore $\dim \operatorname{im} \phi = m$. Hence $\operatorname{im} \phi = F[x]$ and, in particular, $1 \in \operatorname{im} \phi$.

So there is a $v \in F[x]$ with $\phi(v) = 1$. This means $uv = 1$ and $v$ is the multiplicative inverse of $u$. The index $[F[x] : F] = \dim_F F[x] = m$.

Third assume more generally that $E$ is a field, $F \subset E \subset K$, $[E : F] = m$, and $\alpha \in E$ is any element. The elements $1, \alpha, \ldots, \alpha^m$ of $E$ cannot be linearly independent over $F$ since there are $m + 1 > m$ of them. hence there is a dependence relation

$$a_0 + a_1\alpha + \cdots + a_m\alpha^m = 0,$$

that is there is a polynomial $f \in F[X]$ with $f(\alpha) = 0$ and $\deg f \leq m$. Therefore $\alpha$ is algebraic over $F$ and the degree of $\alpha$ is less than or equal to $m$.

Finally, note that for $a$ as in (1), putting these arguments together, we have

$$\text{degree of } x = n \geq m \geq \text{degree of } x.$$

Therefore $m = n =$ the degree of $x$. Thus $\dim F[x] = n$. If the spanning set $1, x, \ldots x^{n-1}$ in the first argument were dependent, a set with fewer than $n$ elements would span $F[x]$ contradicting the fact that its dimension is $n$, so this set is a basis.