and this is the statement of Taylor's formula for the case $f = x^m$. If

$$f = \sum_{m=0}^{n} a_m x^m$$

then

$$D^k f(c) = \sum_m a_m (D^k x^m)(c)$$

and

$$\begin{aligned}\sum_{k=0}^{n} \frac{D^k f(c)}{k!} (x - c)^k &= \sum_k \sum_m a_m \frac{(D^k x^m)}{k!} (c)(x - c)^k \\ &= \sum_m a_m \sum_k \frac{(D^k x^m)}{k!} (c)(x - c)^k \\ &= \sum_m a_m x^m \\ &= f. \quad \blacksquare\end{aligned}$$

It should be noted that because the polynomials $1, (x - c), \ldots, (x - c)^n$ are linearly independent (cf. Exercise 6, Section 4.2) Taylor's formula provides the unique method for writing f as a linear combination of the polynomials $(x - c)^k$ $(0 \leq k \leq n)$.

Although we shall not give any details, it is perhaps worth mentioning at this point that with the proper interpretation Taylor's formula is also valid for polynomials over fields of finite characteristic. If the field F has finite characteristic (the sum of some finite number of 1's in F is 0) then we may have $k! = 0$ in F, in which case the division of $(D^k f)(c)$ by $k!$ is meaningless. Nevertheless, sense can be made out of the division of $D^k f$ by $k!$, because every coefficient of $D^k f$ is an element of F multiplied by an integer divisible by $k!$ If all of this seems confusing, we advise the reader to restrict his attention to fields of characteristic 0 or to subfields of the complex numbers.

If c is a root of the polynomial f, the **multiplicity** of c as a root of f is the largest positive integer r such that $(x - c)^r$ divides f.

The multiplicity of a root is clearly less than or equal to the degree of f. For polynomials over fields of characteristic zero, the multiplicity of c as a root of f is related to the number of derivatives of f that are 0 at c.

Theorem 6. *Let* F *be a field of characteristic zero and* f *a polynomial over* F *with deg* f $\leq$ n. *Then the scalar* c *is a root of* f *of multiplicity* r *if and only if*

$$(D^k f)(c) = 0, \qquad 0 \leq k \leq r - 1$$

$$(D^r f)(c) \neq 0.$$

Proof. Suppose that r is the multiplicity of c as a root of f. Then there is a polynomial g such that $f = (x - c)^r g$ and $g(c) \neq 0$. For other-

wise f would be divisible by $(x - c)^{r+1}$, by Corollary 1 of Theorem 4. By Taylor's formula applied to g

$$f = (x - c)^r \left[\sum_{m=0}^{n-r} \frac{(D^m g)}{m!} (c) (x - c)^m \right]$$

$$= \sum_{m=0}^{n-r} \frac{(D^m g)}{m!} (x - c)^{r+m}$$

Since there is only one way to write f as a linear combination of the powers $(x - c)^k$ $(0 \leq k \leq n)$ it follows that

$$\frac{(D^k f)(c)}{k!} = \begin{cases} 0 \text{ if } 0 \leq k \leq r - 1 \\ \dfrac{D^{k-r} g(c)}{(k - r)!} \text{ if } r \leq k \leq n. \end{cases}$$

Therefore, $D^k f(c) = 0$ for $0 \leq k \leq r - 1$, and $D^r f(c) = g(c) \neq 0$. Conversely, if these conditions are satisfied, it follows at once from Taylor's formula that there is a polynomial g such that $f = (x - c)^r g$ and $g(c) \neq 0$. Now suppose that r is not the largest positive integer such that $(x - c)^r$ divides f. Then there is a polynomial h such that $f = (x - c)^{r+1} h$. But this implies $g = (x - c)h$, by Corollary 2 of Theorem 1; hence $g(c) = 0$, a contradiction. ∎

Definition. *Let* F *be a field. An* **ideal** *in* F[x] *is a subspace* M *of* F[x] *such that* fg *belongs to* M *whenever* f *is in* F[x] *and* g *is in* M.

EXAMPLE 5. If F is a field and d is a polynomial over F, the set $M = dF[x]$, of all multiples df of d by arbitrary f in $F[x]$, is an ideal. For M is non-empty, M in fact contains d. If f, g belong to $F[x]$ and c is a scalar, then

$$c(df) - dg = d(cf - g)$$

belongs to M, so that M is a subspace. Finally M contains $(df)g = d(fg)$ as well. The ideal M is called the **principal ideal generated by** d.

EXAMPLE 6. Let $d_1, \ldots, d_n$ be a finite number of polynomials over F. Then the sum M of the subspaces $d_i F[x]$ is a subspace and is also an ideal. For suppose p belongs to M. Then there exist polynomials $f_1, \ldots, f_n$ in $F[x]$ such that $p = d_1 f_1 + \cdots + d_n f_n$. If g is an arbitrary polynomial over F, then

$$pg = d_1(f_1 g) + \cdots + d_n(f_n g)$$

so that pg also belongs to M. Thus M is an ideal, and we say that M is the ideal **generated** by the polynomials, $d_1, \ldots, d_n$.

EXAMPLE 7. Let F be a subfield of the complex numbers, and consider the ideal

$$M = (x + 2)F[x] + (x^2 + 8x + 16)F[x].$$

We assert that $M = F[x]$. For M contains

$$x^2 + 8x + 16 - x(x + 2) = 6x + 16$$

and hence M contains $6x + 16 - 6(x + 2) = 4$. Thus the scalar polynomial 1 belongs to M as well as all its multiples.

Theorem 7. *If* F *is a field, and* M *is any non-zero ideal in* F[x], *there is a unique monic polynomial* d *in* F[x] *such that* M *is the principal ideal generated by* d.

Proof. By assumption, M contains a non-zero polynomial; among all non-zero polynomials in M there is a polynomial d of minimal degree. We may assume d is monic, for otherwise we can multiply d by a scalar to make it monic. Now if f belongs to M, Theorem 4 shows that $f = dq + r$ where $r = 0$ or deg $r <$ deg d. Since d is in M, dq and $f - dq = r$ also belong to M. Because d is an element of M of minimal degree we cannot have deg $r <$ deg d, so $r = 0$. Thus $M = dF[x]$. If g is another monic polynomial such that $M = gF[x]$, then there exist non-zero polynomials p, q such that $d = gp$ and $g = dq$. Thus $d = dpq$ and

$$\deg d = \deg d + \deg p + \deg q.$$

Hence $\deg p = \deg q = 0$, and as d, g are monic, $p = q = 1$. Thus $d = g$. ∎

It is worth observing that in the proof just given we have used a special case of a more general and rather useful fact; namely, if p is a non-zero polynomial in an ideal M and if f is a polynomial in M which is not divisible by p, then $f = pq + r$ where the 'remainder' r belongs to M, is different from 0, and has smaller degree than p. We have already made use of this fact in Example 7 to show that the scalar polynomial 1 is the monic generator of the ideal considered there. In principle it is always possible to find the monic polynomial generating a given non-zero ideal. For one can ultimately obtain a polynomial in the ideal of minimal degree by a finite number of successive divisions.

Corollary. *If* $p_1, \ldots, p_n$ *are polynomials over a field* F, *not all of which are* 0, *there is a unique monic polynomial* d *in* F[x] *such that*

(a) d *is in the ideal generated by* $p_1, \ldots, p_n$;

(b) d *divides each of the polynomials* p_i.

Any polynomial satisfying (a) *and* (b) *necessarily satisfies*

(c) d *is divisible by every polynomial which divides each of the polynomials* $p_1, \ldots, p_n$.

Proof. Let d be the monic generator of the ideal

$$p_1F[x] + \cdots + p_nF[x].$$

Every member of this ideal is divisible by d; thus each of the polynomials p_i is divisible by d. Now suppose f is a polynomial which divides each of the polynomials $p_1, \ldots, p_n$. Then there exist polynomials $g_1, \ldots, g_n$ such that $p_i = fg_i$, $1 \leq i \leq n$. Also, since d is in the ideal

$$p_1F[x] + \cdots + p_nF[x],$$

there exist polynomials $q_1, \ldots, q_n$ in $F[x]$ such that

$$d = p_1q_1 + \cdots + p_nq_n.$$

Thus

$$d = f[g_1q_1 + \cdots + g_nq_n].$$

We have shown that d is a monic polynomial satisfying (a), (b), and (c). If d' is any polynomial satisfying (a) and (b) it follows, from (a) and the definition of d, that d' is a scalar multiple of d and satisfies (c) as well. Finally, in case d' is a monic polynomial, we have $d' = d$. ∎

Definition. *If* $\mathrm{p}_1, \ldots, \mathrm{p}_n$ *are polynomials over a field* F, *not all of which are* 0, *the monic generator* d *of the ideal*

$$\mathrm{p}_1\mathrm{F}[\mathrm{x}] + \cdots + \mathrm{p}_n\mathrm{F}[\mathrm{x}]$$

is called the **greatest common divisor** (*g.c.d.*) *of* $\mathrm{p}_1, \ldots, \mathrm{p}_n$. *This terminology is justified by the preceding corollary. We say that the polynomials* $\mathrm{p}_1, \ldots, \mathrm{p}_n$ *are* **relatively prime** *if their greatest common divisor is* 1, *or equivalently if the ideal they generate is all of* F[x].

EXAMPLE 8. Let C be the field of complex numbers. Then

(a) g.c.d. $(x + 2, x^2 + 8x + 16) = 1$ (see Example 7);

(b) g.c.d. $((x - 2)^2(x + i), (x - 2)(x^2 + 1)) = (x - 2)(x + i)$. For, the ideal

$$(x - 2)^2(x + i)F[x] + (x - 2)(x^2 + 1)F[x]$$

contains

$$(x - 2)^2(x + i) - (x - 2)(x^2 + 1) = (x - 2)(x + i)(i - 2).$$

Hence it contains $(x - 2)(x + i)$, which is monic and divides both

$$(x - 2)^2(x + i) \quad \text{and} \quad (x - 2)(x^2 + 1).$$

EXAMPLE 9. Let F be the field of rational numbers and in $F[x]$ let M be the ideal generated by

$$(x - 1)(x + 2)^2, \qquad (x + 2)^2(x - 3), \qquad \text{and} \qquad (x - 3).$$

Then M contains

$$\tfrac{1}{2}(x + 2)^2[(x - 1) - (x - 3)] = (x + 2)^2$$

and since

$$(x + 2)^2 = (x - 3)(x + 7) - 17$$

M contains the scalar polynomial 1. Thus $M = F[x]$ and the polynomials

$$(x - 1)(x + 2)^2, \qquad (x + 2)^2(x - 3), \qquad \text{and} \qquad (x - 3)$$

are relatively prime.

Exercises

1. Let Q be the field of rational numbers. Determine which of the following subsets of $Q[x]$ are ideals. When the set is an ideal, find its monic generator.

(a) all f of even degree;
(b) all f of degree ≥ 5;
(c) all f such that $f(0) = 0$;
(d) all f such that $f(2) = f(4) = 0$;
(e) all f in the range of the linear operator T defined by

$$T\left(\sum_{i=0}^{n} c_i x^i\right) = \sum_{i=0}^{n} \frac{c_i}{i+1} x^{i+1}.$$

2. Find the g.c.d. of each of the following pairs of polynomials

(a) $2x^5 - x^3 - 3x^2 - 6x + 4$, $x^4 + x^3 - x^2 - 2x - 2$;
(b) $3x^4 + 8x^2 - 3$, $x^3 + 2x^2 + 3x + 6$;
(c) $x^4 - 2x^3 - 2x^2 - 2x - 3$, $x^3 + 6x^2 + 7x + 1$.

3. Let A be an $n \times n$ matrix over a field F. Show that the set of all polynomials f in $F[x]$ such that $f(A) = 0$ is an ideal.

4. Let F be a subfield of the complex numbers, and let

$$A = \begin{bmatrix} 1 & -2 \\ 0 & 3 \end{bmatrix}.$$

Find the monic generator of the ideal of all polynomials f in $F[x]$ such that $f(A) = 0$.

5. Let F be a field. Show that the intersection of any number of ideals in $F[x]$ is an ideal.

6. Let F be a field. Show that the ideal generated by a finite number of polynomials $f_1, \ldots, f_n$ in $F[x]$ is the intersection of all ideals containing $f_1, \ldots, f_n$.

7. Let K be a subfield of a field F, and suppose f, g are polynomials in $K[x]$. Let M_K be the ideal generated by f and g in $K[x]$ and M_F be the ideal they generate in $F[x]$. Show that M_K and M_F have the same monic generator.

4.5. The Prime Factorization of a Polynomial

In this section we shall prove that each polynomial over the field F can be written as a product of 'prime' polynomials. This factorization provides us with an effective tool for finding the greatest common divisor