Greatest common divisor

Let $\varphi(x), f(x), g(x)$ be polynomials in $\mathbb{F}[x]$. If $\varphi(x)$ divides both $f(x)$ and $g(x)$, then $\varphi(x)$ is called a common divisor of $f(x)$ and $g(x)$.

Def 1 Let $f(x)$ and $g(x)$ be two polynomials in $\mathbb{F}[x]$. A polynomial $d(x)$ in $\mathbb{F}[x]$ is called a greatest common divisor of $f(x)$ and $g(x)$, if it satisfies the following conditions: g.c.d.

(i) $d(x)$ is a common divisor of $f(x)$ and $g(x)$; $d(x)\mid f(x)$, $d(x)\mid g(x)$

(ii) $d(x)$ is divisible by every common divisor of $f(x)$ and $g(x)$.

If $\varphi(x)\mid f(x)$ and $\varphi(x)\mid g(x)$, then $\varphi(x)\mid d(x)$.

For example, for arbitrary polynomial $f(x)$, $f(x)$ is a greatest common divisor of $f(x)$ and 0; If $g(x)\mid f(x)$, then $g(x)$ is a greatest common divisor of $f(x)$ and $g(x)$.

Lemma 1. If $f(x)=q(x)g(x)+r(x)$, then the list of common divisors of $f(x)$ and $g(x)$ coincides with the list of common divisors of $g(x)$ and $r(x)$.

(Here insert the Euclidean Algorithm)

Theorem 1 (Bézout). For any polynomials $f(x)$ and $g(x)$ in $\mathbb{F}[x]$, there exists a greatest common divisor $d(x)$ in $\mathbb{F}[x]$, and $d(x)$ can be represented as a linear combination of $f(x)$ and $g(x)$, namely, there exist polynomials $u(x)$ and $v(x)$ in $\mathbb{F}[x]$ such that

$$d(x)=u(x)f(x)+v(x)g(x).$$ (Bézout's identity)

Example. For the pair of polynomials $f(x)$ and $g(x)$ below, use the Euclidean algorithm to find polynomials $u(x)$ and $v(x)$ such that $u(x)f(x)+v(x)g(x)$ equals a greatest common divisor of $f(x)$ and $g(x)$:

① $f(x)=x^5+1$ and $g(x)=x^2+1$ in $\mathbb{Q}[x]$;

② $f(x)=x^4+3x^3-x^2-4x-3$, and $g(x)=3x^3+10x^2+2x-3$ in $\mathbb{C}[x]$. (Exercise)

Euclidean Algorithm: Given two polynomials $f(x)$ and $g(x)$ with $g(x) \neq 0$, divide g into f, then the remainder into g, then that remainder into the previous remainder, etc, or symbolically,

$$f(x) = q_1(x)\, g(x) + r_1(x)$$
$$g(x) = q_2(x)\, r_1(x) + r_2(x)$$
$$r_1(x) = q_3(x)\, r_2(x) + r_3(x)$$
$$\vdots$$
$$r_{k-2}(x) = q_k(x)\, r_{k-1}(x) + r_k(x)$$
$$r_{k-1}(x) = q_{k+1}(x)\, r_k(x) + 0$$

Since $\deg r_1(x) < \deg g(x)$, $\deg r_2(x) < \deg r_1(x)$, etc., the sequence of divisions ends after at most $\deg g(x) = k$ steps. Then we have

Theorem: In Euclid's Algorithm for $f(x)$ and $g(x)$, the last nonzero remainder $r_k(x)$ is a greatest common divisor of f and g.

Example. Find a greatest common divisor of $f(x)$ and $g(x)$ by Euclid's Algorithm, where $f(x) = x^5+1$ and $g(x) = x^2+1$ in $\mathbb{Q}[x]$.

Solution: $f(x) = x^5+1 = (x^3-x)\, g(x) + (x+1)$

$$g(x) = (x-1)(x+1) + 2$$
$$x+1 = \tfrac{1}{2}(x+1)\cdot 2 + 0$$

This gives that 2 is a greatest common divisor of $f(x)$ and $g(x)$. □

Answers.

(1) By the Euclidean algorithm, we have the following sequence of equalities:

$$f(x) = x^5+1 = (x^3-x)g(x) + \underbrace{(x+1)}_{r_1}$$

$$g(x) = x^2+1 = (x-1)\underbrace{(x+1)}_{r_1} + \underbrace{2}_{r_2}$$

$$\underbrace{x+1}_{r_1} = \left(\tfrac{1}{2}x+\tfrac{1}{2}\right)\times \underbrace{2}_{r_2} + 0$$

The last nonzero remainder is 2. Thus 2 is a greatest common divisor of $f(x)=x^5+1$ and $g(x)=x^2+1$. Bézout theorem asserts in this case 2 is a linear combination of x^5+1 and x^2+1. Indeed, we have

$$\begin{aligned} 2 &= g(x) - (x-1)(x+1) \\ &= g(x) - (x-1)\left[f(x) - (x^3-x)g(x)\right] \\ &= \left((x-1)(x^3-x)+1\right)g(x) - (x-1)f(x) \end{aligned}$$

Hence we can take

$$u(x) = -(x-1) \quad \text{and} \quad v(x) = (x-1)(x^3-x)+1$$

which satisfy

$$2 = u(x)f(x) + v(x)g(x).$$

(2) $|9x+27|$ is a greatest common divisor of $f(x)$ and $g(x)$. And

$$|9x+27| = u(x)f(x) + v(x)g(x)$$

where $u(x) = \frac{27}{5}x - 9$ and $v(x) = -\frac{9}{5}x^2 + \frac{18}{5}x$.

The greatest common divisor is determined up to a nonzero constant multiple.

Remark: The greatest common divisors of two polynomials $f(x)$ and $g(x)$ are all non-zero constant multiples of each other. We use (f,g) or $(f(x),g(x))$ to denote the greatest common divisor with leading coefficient 1. (Uniquely determined)

For instance, if $|9x+27|$ is a g.c.d. of $f(x)$ and $g(x)$, then

$$(f,g) = x+3.$$

Def2 If the greatest common divisor of two polynomials $f(x)$ and $g(x)$ is equal to 1, then $f(x)$ and $g(x)$ are said to be relatively prime or coprime.

Thm2 Let $f(x)$ and $g(x)$ be in $F[x]$. $f(x)$ and $g(x)$ are coprime if and only if there exist $u(x), v(x) \in F[x]$ such that

$$u(x)f(x) + v(x)g(x) = 1$$

proof: It suffices to prove the sufficiency. suppoe that $d(x)$ is a greatest common divisor of $f(x)$ and $g(x)$. Then $d(x) | f(x)$ and $d(x) | g(x)$. Thus $d(x)$ divides 1. This implies $d(x)$ is a non-zero constant. Hence, $f(x)$ and $g(x)$ are coprime. □

Corollary 1 If $(f(x), g(x)) = 1$ and $f(x) | g(x)h(x)$, then $f(x) | h(x)$.

proof: There exist $u(x)$ and $v(x)$ such that

$$u(x)f(x) + v(x)g(x) = 1.$$

Then multiplying both sides of the equation by $h(x)$ yields

$$u(x)f(x)h(x) + v(x)g(x)h(x) = h(x).$$

It follows $f(x) | h(x)$, since $f(x)$ divides the left-hand side of the equation. □.

Corollary 2 If $f_1(x) | g(x)$, $f_2(x) | g(x)$ and $(f_1(x), f_2(x)) = 1$, then $f_1(x)f_2(x) | g(x)$.

proof: By $f_1(x) | g(x)$, there exists $h(x)$ such that

$$g(x) = f_1(x)h(x)$$

Now $f_2(x) | f_1(x)h(x)$ and $(f_1(x), f_2(x)) = 1$, thus $f_2(x) | h(x)$. There exists $h_2(x)$ such that

$$h(x) = f_2(x)h_2(x)$$

This gives $g(x) = f_1(x)f_2(x)h_2(x)$ and thus $f_1(x)f_2(x) | g(x)$. □

Generalizations to more than two polynomials.

Def3. Let $f_1(x), f_2(x), \cdots, f_s(x)$ $(s \geq 2)$ be polynomials in $F[x]$. A polynomial $d(x)$ in $F[x]$ is called a greatest common divisor of $f_1, f_2, \cdots, f_s$ if it satisfies

1) $d(x) \mid f_i(x)$, $1 \leq i \leq s$;

2) if $h(x) \mid f_i(x)$, $1 \leq i \leq s$, then $h(x) \mid d(x)$.

We still use $(f_1, f_2, \cdots, f_s)$ to denote the greatest common divisor whose leading coefficient is equal to 1. If $f_1(x), \cdots, f_s(x)$ are non-zero polynomials, then

$$(f_1, f_2, \cdots, f_s) = ((f_1, f_2, \cdots, f_{s-1}), f_s).$$

Furthermore, there exist polynomials $u_i(x)$, $1 \leq i \leq s$, such that

$$u_1(x)f_1(x) + u_2(x)f_2(x) + \cdots + u_s(x)f_s(x) = (f_1, f_2, \cdots, f_s).$$

Def4. Polynomials $f_1(x), \cdots, f_s(x)$ $(s \geq 2)$ whose greatest common divisor $(f_1, f_2, \cdots, f_s)$ is equal to 1 are said to be relatively prime or coprime.

Homework:

P29. 5, 6, 7, 8, 9, 10, 11, 12, 13, 14.

Appendix (I) The method of mathematical induction

Theorem 1. (Induction) Fix an integer n_0 and let $P(n)$ be a statement which makes sense for every integer $n \geq n_0$. Then $P(n)$ is true for all $n \geq n_0$, if the following two statements are true:

(a) $P(n_0)$ is true;

(b) for all $k \geq n_0$, if $P(k)$ is true, then $P(k+1)$ is true.

When using induction to prove a theorem, proving (a) is called the base case, and proving (b) is called the induction step.

~~proof: Let $sp(n)$ be ...~~

Example 1. For all $n \geq 1$, $1+3+5+\cdots+(2n-1)=n^2$.

proof: Let $P(n)$ be the statement

$$1+3+5+\cdots+(2n-1)=n^2$$

The base case $P(1)$ is true, since $1=1^2$. For the induction step, let k be some unspecified number ≥ 1, and assume that $P(k)$ is true, that is,

$$1+3+5+\cdots+(2k-1)=k^2.$$

We want to show that then $P(k+1)$ is true, that is,

$$1+3+\cdots+(2k-1)+(2k+1)=(k+1)^2.$$

To do so, we can add $(2k+1)$ to both sides of the equation $P(k)$ to get

$$1+3+\cdots+(2k-1)+(2k+1)=k^2+(2k+1)=(k+1)^2$$

Thus, assuming $P(k)$ is true, it follows that $P(k+1)$ is true.

By induction, $P(n)$ is true for all ~~$n \geq 1$~~ $n \geq 1$. □

Theorem 2 (Complete Induction) Let n_0 be a fixed integer and let $P(n)$ be a statement which makes sense for every integer $n \geq n_0$. Then $P(n)$ is true for all integers $n \geq n_0$, if the following two statement are true:

(a) (base case) $P(n_0)$ is true;

(b) (induction step) For all $m > n_0$, if $P(k)$ is true for all $n_0 \leq k < m$, then $P(m)$ is true.

Example 2 Every natural number $n \geq 2$ is divisible by a prime number.

Proof. Let $P(n)$ be the statement "n is divisible by a prime number, where $n \geq 2$." Then the base case $P(2)$ is true, because 2 is prime and 2 divides itself. We'll use complete induction for the induction step. Thus we assume $P(k)$ is true for all k where $2 \leq k < m$: that is, we assume that every natural number ≥ 2 and $< m$ is divisible by a prime number. Now consider m. If m is prime, then m is divisible by a prime number, namely, itself, and $P(m)$ is true. If m is not prime, then m factors as $m = ab$, where $2 \leq a < m$ and also $2 \leq b < m$. Since $2 \leq a < m$, by assumption $P(a)$ is true, that is, a is divisible by a prime. Since a is divisible by a prime, and a divides m, m is divisible by the same prime. So $P(m)$ is true.

Thus $P(n)$ is true for all $n \geq 2$ by Complete Induction. □

§5. Factorization

Example 1. In $\mathbb{Q}[x]$, we have

$$x^4-4=(x^2-2)(x^2+2)$$

In $\mathbb{Q}[\sqrt{2}][x]$ or $\mathbb{R}[x]$, we have

$$x^4-4=(x^2-2)(x^2+2)=(x-\sqrt{2})(x+\sqrt{2})(x^2+2)$$

In $\mathbb{C}[x]$, we have

$$x^4-4=(x-\sqrt{2})(x+\sqrt{2})(x-\sqrt{2}i)(x+\sqrt{2}i)$$

Definition 1. Let $p(x)$ be a polynomial over the $\mathbb{F}[x]$ of degree ≥ 1. $p(x)$ is called an irreducible polynomial (or prime polynomial) if there exists no factorization $p(x)=r(x)s(x)$, where $r(x), s(x)\in\mathbb{F}[x]$ and both $r(x)$ and $s(x)$ are of degree ≥ 1. [Otherwise, $p(x)$ is said to be reducible. Namely, there exists polynomials $r(x)$ and $s(x)$ in $\mathbb{F}[x]$ of degree ≥ 1 such that $f(x)=r(x)s(x)$.]

Example 2. Linear polynomials are irreducible.

Remark 1. (1) Whether a polynomial is irreducible depends on the field $\mathbb{F}$. (see example 1).

(2) The irreducible polynomials of $\mathbb{F}[x]$ are those polynomials $f(x)$ of positive degree, that are only divisible by units of $\mathbb{F}[x]$ and by associates of $f(x)$, i.e. polynomials of the form $cf(x)$ with $0\neq c\in\mathbb{F}$.

(3) If $p(x)$ is irreducible and $f(x)$ is a polynomial which is not divisible by $p(x)$, then $(p(x), f(x))=1$.

proof: Suppose $d(x)=(p(x), f(x))$, then $d(x)\mid p(x)$. since $p(x)$ is irreducible, $d(x)$ is a unit or $d(x)=cp(x)$ for some nonzero constant c. In the latter case, $p(x)\mid f(x)$, which contradicts the assumption. Hence $d(x)$ is a unit. □.

Theorem 1 Let $p(x)$ be an irreducible polynomial in $\mathbb{F}[x]$, $\mathbb{F}$ a field. For any polynomials $f(x), g(x) \in \mathbb{F}[x]$, if $p(x) \mid f(x)g(x)$, then $p(x) \mid f(x)$ or $p(x) \mid g(x)$.

Proof If $p(x) \nmid f(x)$, then $(p(x), f(x)) = 1$. By $p(x) \mid f(x)g(x)$, we have $p(x) \mid g(x)$. □.

Remark 2 The result applies when we have more than two polynomials. For example, Let $p(x), f_1(x), \ldots, f_s(x)$ are polynomials in $\mathbb{F}[x]$, with $p(x)$ irreducible. If $p(x)$ divides the product of $f_1(x), \ldots, f_s(x)$, then $p(x)$ must divide one of them. (Homework: prove it)

The following is the theorem on factorization.

Theorem 2 Let $\mathbb{F}$ be a field. Every polynomial of degree ≥ 1 over $\mathbb{F}$ is irreducible or factors into a product of irreducible polynomials.

Proof Let f be a polynomial of degree n, with $n \geq 1$. We use induction on n. If $n=1$, then f is irreducible and thus the statement is true for $n=1$. For $n>1$, suppose the statement is true for all $1<k<n$, that is every polynomial of degree k with $1 \leq k < n$ is irreducible or factors into a product of irreducible polynomials. Now consider n. If f is irreducible, then the statement holds. If not, f can be factored into a product of two polynomials of degree ≥ 1. Say $f = g(x)h(x)$, $1 \leq \deg g(x) < n$ and $1 \leq \deg h(x) < n$. By the induction assumption, $g(x) = p_1(x)p_2(x)\cdots p_r(x)$, a product of irreducible polynomials, and also $h(x) = q_1(x)q_2(x)\cdots q_s(x)$, a product of irreducible polynomials. So $f = p(x)p_2\cdots p_r(x)q_1(x)q_2(x)\cdots q_s(x)$ is a product of irreducible polynomials.

By complete induction, the statement is true for all polynomials of positive degree. □.

Here is the theorem on uniqueness of factorization:

Theorem 3. Let F be a field. In $F[x]$, if

$$f(x)=p_1(x)p_2(x)\cdots p_s(x)=q_1(x)q_2(x)\cdots q_t(x) \qquad (1).$$

are two factorizations of the polynomial $f(x)$ into a product of irreducible polynomials in $F[x]$, then $s=t$ and there is a one to one correspondence between the factors $p_1(x), p_2(x), \ldots, p_s(x)$ and $q_1(x), q_2(x), \ldots, q_t(x)$, where if $p_i(x)$ corresponds with $q_j(x)$, then $p_i(x)$ and $q_j(x)$ are associates.

proof. Induction on s. For $s=1$, $f(x)=p_1(x)$ is irreducible. Thus $t=1$ and $p_1(x)=q_1(x)$.

Suppose that ~~the statement holds~~ have proved the theorem for $s-1$. Now consider s. It follows from (1) that

$$p_1(x) \mid q_1(x)q_2(x)\cdots q_t(x).$$

Since $p_1(x)$ is irreducible, $p_1(x)$ must divide some $q_i(x)$. ~~As $q_i(x)$ is irreducible, $p_1(x)=c_i q_i(x)$ for some nonzero constant $c_i \in F$. Substituting this into (1) and by cancellation law, we get~~

Without loss of generality, $p_1(x) \mid q_1(x)$. As $q_1(x)$ is irreducible, $p_1(x)=c_1 q_1(x)$ with $0 \neq c_1 \in F$. Substituting this back into (1) and by cancellation law, we get

$$c_1 p_2(x)\cdots p_s(x)=q_2(x)\cdots q_t(x) \qquad (2)$$

Since the number of irreducible polynomials on the left-hand side of (2) is $s-1$, our inductive assumption applies and there is a one to one correspondence between the factors $c_1p_2, p_3, \ldots, p_s(x)$ and $q_2(x), \ldots, q_t(x)$, and $s-1=t-1$. Thus $s=t$. This together with $p_1(x)=c_1 q_1(x)$ shows that the theorem is true for s.

By induction, the theorem is true. □

Remark:

(1) We can write the irreducible factorization of a polynomial $f(x)$ of degree ≥ 1 in $\mathbb{F}[x]$ in exponential notation, as

$$f = p_1(x)^{e_1} p_2(x)^{e_2} \cdots p_s(x)^{e_s} \quad (2)$$

where $p_1(x), p_2(x), \ldots, p_s(x)$ are distinct irreducible polynomials and $e_1 + \cdots e_s = \deg f$. If any e_i is bigger than 1, we shall say that f has a multiple factor. For example, $f(x) = (x^2+2)^3(2x+1)$ in $\mathbb{R}[x]$ has a multiple factor, while $f(x) = (x^2+2)(2x+1)$ does not has any multiple factor.

(2) Since any polynomial is an associate of a unique monic polynomial, we can rewrite (2) as

$$f(x) = a\, q_1(x)^{e_1} q_2(x)^{e_2} \cdots q_s(x)^{e_s} \quad \text{(normalized factorization)} \quad (3)$$

where $q_1(x), \ldots, q_s(x)$ are distinct monic irreducible polynomials, a is a nonzero element of $\mathbb{F}$ (the leading coefficient of $f(x)$), and $e_1, \ldots, e_s$ are positive integers with $e_1 + \cdots + e_s = \deg f$. Such a factorization is called a normalized factorization of $f(x)$.

(3) If the factorization of f and g into products of irreducible polynomial are given in exponential notation, then it is easy to write down the greatest common divisor of f and g, and least common multiple of f and g.

Example: Find the greatest common divisor in $\mathbb{Q}[x]$ of $f(x) = (x^2-3x-4)^3(x-3)^2$ and $g(x) = (x-4)^3(x^2-3x-4)^2$

Solution: $(x-4)(x+1)$ is the g.c.d. of $f(x)$ and $g(x)$. □

Here is the theorem on uniqueness of factorization:

Theorem 3. Let F be a field. In $F[x]$, if

$$f(x)=p_1(x)p_2(x)\cdots p_s(x)=q_1(x)q_2(x)\cdots q_t(x) \qquad (1).$$

are two factorizations of the polynomial $f(x)$ into a product of irreducible polynomials in $F[x]$, then $s=t$ and there is a one-to-one correspondence between the factors $p_1(x), p_2(x), \ldots, p_s(x)$ and $q_1(x), q_2(x), \ldots, q_t(x)$, where if $p_i(x)$ corresponds with $q_j(x)$, then $p_i(x)$ and $q_j(x)$ are associates.

proof. Induction on s. For $s=1$, $f(x)=p_1(x)$ is irreducible. Thus $t=1$ and $p_1(x)=q_1(x)$. Suppose that ~~the statement holds~~ we have proved the theorem for $s-1$. Now consider s. It follows from (1) that

$$p_1(x) \mid q_1(x)q_2(x)\cdots q_t(x).$$

Since $p_1(x)$ is irreducible, $p_1(x)$ must divide some $q_i(x)$, $1\le i\le t$. ~~As $q_i(x)$ is irreducible, $p_1(x)=c_i q_i(x)$ for some nonzero constant $c_i\in F$. Substituting this into (1) and by cancellation law, we get~~

Without loss of generality, $p_1(x)\mid q_1(x)$. As $q_1(x)$ is irreducible, $p_1(x)=c_1q_1(x)$ with $0\neq c_1\in F$. Substituting this back into (1) and by cancellation law, we get

$$c_1p_2(x)\cdots p_s(x)=q_2(x)\cdots q_t(x) \qquad (2)$$

Since the number of irreducible polynomials on the left-hand side of (2) is $s-1$, our inductive assumption applies and there is a one-to-one correspondence between the factors $c_1p_2, p_3, \ldots, p_s(x)$ and $q_2(x), \ldots, q_t(x)$, and $s-1=t-1$. Thus $s=t$. This together with $p_1(x)=c_1q_1(x)$ shows that the theorem is true for s.

By induction, the theorem is true. □

Remarks.

(1) We can write the irreducible factorization of a polynomial $f(x)$ of degree ≥ 1 in $\mathbb{F}[x]$ in exponential notation, as

$$f = p_1(x)^{e_1} p_2(x)^{e_2} \cdots p_s(x)^{e_s} \qquad (2)$$

where $p_1(x), p_2(x), \ldots, p_s(x)$ are distinct irreducible polynomials. If any e_i is bigger than 1, we shall say that f has a multiple factor. For example, $f(x) = (x^2+2)^3(2x+1)$ in $\mathbb{R}[x]$ has a multiple factor, while $f(x) = (x^2+2)(2x+1)$ does not has any multiple factor.

(2) Since any polynomial is an associate of a unique monic polynomial, we can rewrite (2) as

$$f(x) = a\, q_1(x)^{e_1} q_2(x)^{e_2} \cdots q_s(x)^{e_s} \qquad \text{(normalized factorization)} \qquad (3)$$

where $q_1(x), \ldots, q_s(x)$ are distinct monic irreducible polynomials, a is a nonzero element of $\mathbb{F}$ (the leading coefficient of $f(x)$), and $e_1, \ldots, e_s$ are positive integers. Such a factorization is called a normalized factorization of $f(x)$.

(3) If the factorization of f and g into products of irreducible polynomials are given in exponential notation, then it is easy to write down the greatest common divisor of f and g, and least common multiple of f and g.

Example: Find the greatest common divisor in $\mathbb{Q}[x]$ of $f(x) = (x^2-3x-4)^3(x-3)^2$ and $g(x) = (x-4)^3(x^2-3x-4)^2$

Solution: $(x-4)(x+1)$ is the g.c.d. of $f(x)$ and $g(x)$. □

§6. Multiple factors

Def 1. An irreducible polynomial $p(x)$ is called a factor of a polynomial $f(x)$ of multiplicity k, if $p^k(x) \mid f(x)$, $p^{k+1}(x) \nmid f(x)$, where k is a positive integer. If $k=1$, we say $p(x)$ is a simple factor of $f(x)$; if $k>1$, we say $p(x)$ is a multiple factor of $f(x)$.

Remark 1. The multiplicity of $p(x)$ as a factor of $f(x)$ is the largest positive integer k such that $p(x)^k$ divides $f(x)$. The multiplicity k is clearly less than or equal to the degree of $f(x)$.

Example. Write $f(x)$ as a standard/normalized factorization

$$f(x) = a\, p_1(x)^{r_1} p_2(x)^{r_2} \cdots p_s(x)^{r_s}.$$

When $r_i > 1$, then $p_i(x)$ is a multiple factor of multiplicity r_i.

The formal derivatives of a polynomial are useful in discussing multiple factors.

Def 2. The derivative of the polynomial

$$f(x) = a_n x^n + \cdots + a_1 x + a_0$$

is the polynomial

$$f'(x) = n a_n x^{n-1} + \cdots + a_1$$

We also use the notation $Df = f'$. We have the higher order formal derivatives

$$Df'(x) = f''(x),\quad f^{(3)} = Df''(x) = D^3 f(x), \text{ and so on.}$$

proposition 1. Let $f(x)$ and $g(x)$ be in $\mathbb{F}[x]$ and let $c \in \mathbb{F}$. Then

(1) $(cf(x))' = cf'(x)$, (2) $(f(x)+g(x))' = f'(x)+g'(x)$,

(3) $(f(x)g(x))' = f'(x)g(x) + f(x)g'(x)$, (4) $(f^m(x))' = m f^{m-1}(x) f'(x)$.

"product rule" "power rule"

Leave the proof of proposition as a homework.

Now we determine the polynomial whose derivative is the zero polynomial.

$$f(x) = a_m x^m + \cdots + a_1 x + a_0$$

$$f'(x) = m a_m x^{m-1} + \cdots + a_1$$

Hence $f'(x) = 0$ if and only if $n a_n = 0$ for $1 \le n \le m$, namely, $a_n = 0$, $1 \le n \le m$.

That is, $f'(x) = 0$ if and only if $f(x) = a_0$, i.e. $f(x)$ is a constant polynomial.

Fact: If $\deg f = n$, then $f^{(n)}(x) = n! a_n$ and $f^{(n+1)}(x) = 0$, and $\deg f' = n-1$.

Thm 1. Let $p(x)$ be irreducible factor of the polynomial $f(x)$ of multiplicity k, with $k \ge 1$. Then $p(x)$ is a factor of $f'(x)$ of multiplicity $k-1$. In particular, if $k=1$, then $f'(x)$ is not divisible by $p(x)$.

proof: By assumption, $f(x) = p^k(x) g(x)$, where $p(x) \nmid g(x)$. We have

$$\begin{aligned} f'(x) &= (p^k(x))' g(x) + p^k(x) g'(x) \\ &= k p^{k-1}(x) p'(x) g(x) + p^k(x) g'(x) \\ &= p^{k-1}(x) [k p'(x) g(x) + p(x) g'(x)] \end{aligned}$$

It suffices to show the polynomial in square brackets is not divisible by $p(x)$. If $p(x)$ did divide this polynomial, then it would also divide $kp'(x)g(x)$, but this is impossible, since $g(x)$ is not divisible by $p(x)$, and $\deg(kp'(x)) < \deg(p(x))$. □.

(Here insert the corollary 2)

Thm 2. An irreducible polynomial $p(x)$ is a multiple factor of $f(x)$ if and only if $p(x)$ is a common factor of $f(x)$ and $f'(x)$.

proof: $\Rightarrow$ Suppose $f(x) = p^k(x) h(x)$ with $k > 1$. Then using the product and power rules,

$$\begin{aligned} f'(x) &= (p^k(x))' h(x) + p^k(x) h'(x) \\ &= p^{k-1}(x) [k p'(x) g(x) + p(x) g'(x)] \end{aligned}$$

so that if $k > 1$, then $q(x)$ is a common factor of $f(x)$ and $f'(x)$.

Leave the proof of proposition as a homework.

Now we determine the polynomial whose derivative is the zero polynomial.

$$f(x)=a_m x^m+\cdots+a_1x+a_0$$

$$f'(x)=m a_m x^{m-1}+\cdots+a_1$$

Here $f'(x)=0$ if and only if $n a_n=0$ for $1\le n\le m$, namely, $a_n=0$, $1\le n\le m$.

That is, $f'(x)=0$ if and only if $f(x)=a_0$, i.e. $f(x)$ is a constant polynomial.

Fact: If $\deg f=n$, then $f^{(n)}(x)=n!\,a_n$ and $f^{(n+1)}(x)=0$, and $\deg f'=n-1$.

Thm1. Let $p(x)$ be irreducible factor of the polynomial $f(x)$ of multiplicity k, with $k\ge 1$. Then $p(x)$ is a factor of $f'(x)$ of multiplicity $k-1$. In particular, if $k=1$, then $f'(x)$ is not divisible by $p(x)$.

proof: By assumption, $f(x)=p^k(x)g(x)$, where $p(x)\nmid g(x)$. We have

$$\begin{aligned} f'(x)&=(p^k(x))'g(x)+p^k(x)g'(x)\\ &=k\,p^{k-1}(x)p'(x)g(x)+p^k(x)g'(x)\\ &=p^{k-1}(x)[kp'(x)g(x)+p(x)g'(x)] \end{aligned}$$

It suffices to show the polynomial in square brackets is not divisible by $p(x)$. If $p(x)$ did divide this polynomial, then it would also divide $kp'(x)g(x)$, but this is impossible, since $g(x)$ is not divisible by $p(x)$, and $\deg(kp'(x))<\deg(p(x))$. □.

(Here insert the corollary 2)

Thm2. An irreducible polynomial $p(x)$ is a multiple factor of $f(x)$ if and only if $p(x)$ is a common factor of $f(x)$ and $f'(x)$.

proof: $\Rightarrow$ Suppose $f(x)=p^k(x)h(x)$ with $k>1$. Then using the product and power rules,

$$\begin{aligned} f'(x)&=(p^k(x))'h(x)+p^k(x)h'(x)\\ &=p^{k-1}(x)[kp'(x)g(x)+p(x)g'(x)] \end{aligned}$$

so that if $k>1$, then $q(x)$ is a common factor of $f(x)$ and $f'(x)$.

$\Leftarrow$ Suppose $p(x)$ is an irreducible common ~~divi~~ factor of $f(x)$ and $f'(x)$. Then $f(x) = p(x)h(x)$ for some polynomial $h(x)$. So by the product rule,

$$f'(x) = p'(x)h(x) + p(x)h'(x).$$

Since $p(x) \mid f'(x)$, $p(x)$ must divide $p'(x)h(x)$. Since $p(x)$ is irreducible, $p(x)$ must divide $p'(x)$ or $h(x)$. If $p(x) \mid p'(x)$, then $p'(x) = 0\,p(x) + p'(x)$ gives that $p'(x) = 0$, Thus $p(x)$ is a constant. This is impossible since $p(x)$ is irreducible. Hence $p(x) \mid h(x)$. Then $h(x) = p(x)g(x)$ for some $g(x)$ and so

$$f(x) = p^2(x)g(x),$$

and $p(x)$ is a multiple factor of $f(x)$, proving the theorem. □.

Corollary 1. $f(x)$ has no multiple factors if and only if $f(x)$ and $f'(x)$ are relatively prime.

The following is a direct corollary of Theorem 1.

Corollary 2. Let $p(x)$ be a multiple irreducible factor of $f(x)$ of multiplicity k $(k \geq 1)$. Then $p(x)$ is a factor of $f(x), f'(x), \cdots, f^{(k-1)}(x)$, but $p(x)$ is not a factor of $f^{(k)}(x)$.

proof: Induction k. By the proof of Theorem 1, the corollary holds for $k=1$. Suppose that the corollary is true for k and suppose that $p(x)$ is a multiple irreducible factor of $f(x)$ of multiplicity $k+1$. By Theorem 1, $p(x)$ is a multiple factor of $f'(x)$ of multiplicity k. By the inductive assumption, $p(x)$ is a factor of $f'(x), f''(x), \ldots, f^{(k)}(x) = (f')^{(k)}(x)$, but not a factor of $(f')^{(k+1)}(x) = f^{(k+1)}(x)$. Hence, $p(x)$ is a factor of $f(x), f'(x), \ldots, f^{(k)}(x)$, but not a factor of $f^{(k+1)}(x)$. □

Example: Let $f(x)=x^3+x^2-8x-12$ be in $\mathbb{Q}[x]$. Then $f'(x)=3x^2+2x-8$. Doing Euclidean algorithm on f and f' gives

$$f(x)=\left(\frac{1}{3}x+\frac{1}{9}\right)f'(x)+\left(-\frac{50}{9}x-\frac{100}{9}\right).$$

Then dividing $f'(x)$ by $x+2$, we get

$$f'(x)=(x+2)(3x-4).$$

So $x+2$ is the greatest common divisor of f and f'. Hence $x+2$ is a multiple factor of $f(x)$. If we divide $f(x)$ by $(x+2)^2$, we obtain

$$f(x)=(x+2)^2(x-3).$$

Hence we factor $f(x)$ into a product of irreducible polynomials.

Remark: Consider the normalized factorization of $f(x)$:

$$f(x)=a\,p_1(x)^{r_1}p_2(x)^{r_2}\cdots p_s(x)^{r_s}$$

where $p_1(x), p_2(x), \ldots, p_s(x)$ are distinct irreducible factors of $f(x)$. Then for each i, the highest power of $p_i(x)$ that divides $f'(x)$ is $p_i(x)^{r_i-1}$, and so the greatest common divisor of $f(x)$ and $f'(x)$ is

$$(f(x),f'(x))=p_1(x)^{r_1-1}p_2(x)^{r_2-1}\cdots p_s(x)^{r_s-1}.$$

Hence,

$$\frac{f(x)}{(f(x),f'(x))}=a\,p_1(x)\,p_2(x)\cdots p_s(x)$$

which is called the **square free part** of $f(x)$. It is obvious that $f(x)$ and $\frac{f(x)}{(f(x),f'(x))}$ have the same irreducible factors in $F[x]$, except that in $\frac{f(x)}{(f(x),f'(x))}$ all the irreducible factor have multiplicity 1.

§7. polynomial function

A field E that contains $\mathbb{F}$ as a subfield is called an extension field of $\mathbb{F}$. Clearly, a polynomial $f(x)$ in $\mathbb{F}[x]$ can be also regarded as a polynomial in $E[x]$.

Let $f(x)=a_n x^n+a_{n-1}x^{n-1}+\cdots+a_0 \in \mathbb{F}[x]$, and $\alpha \in E$. By substituting α for x, we obtain

$$f(\alpha)=a_n\alpha^n+a_{n-1}\alpha^{n-1}+a_1\alpha+a_0 \in E,$$

which is called the value of $f(x)$ at $x=\alpha$. Hence, we may define a polynomial function $\tilde{f}: E \to E$ by letting for every $\alpha \in E$,

$$\tilde{f}(\alpha)=f(\alpha)=a_n\alpha^n+a_{n-1}\alpha^{n-1}+\cdots+a_1\alpha+a_0.$$

Therefore, $\tilde{f}$ is determined by the polynomial $f(x)$. By abuse of notation, we also denote $\tilde{f}$ by f sometime.

Facts. Let $f(x), g(x)$ be in $\mathbb{F}[x]$. If $f(x)+g(x)=h(x)$ and $f(x)g(x)=k(x)$, then

$$f(\alpha)+g(\alpha)=h(\alpha),\quad f(\alpha)g(\alpha)=k(\alpha),\quad \forall\ \alpha \in E.$$

Definition 1. We shall say a number α is a root of $f(x)$, if $f(\alpha)=0$.

Theorem 1. (Remainder Theorem) When dividing $f(x)$ by $x-\alpha$, then the remainder is equal to $f(\alpha)$.

proof: By Euclidean algorithm, there exist $q(x)$ and a number r such that

$$f(x)=q(x)(x-\alpha)+r$$

It follows that $f(\alpha)=q(\alpha)(\alpha-\alpha)+r=r$.

Corollary 1. α is a root of $f(x)$ if and only if $x-\alpha$ divides $f(x)$.

Hence if α is a root of $f(x)$, then there exists $f_1(x) \in \mathbb{F}[x]$ such that

$$f(x) = (x-\alpha) f_1(x).$$

If the factor $f_1(x)$ in $f(x)=(x-\alpha)f_1(x)$ has again the root α, then we obtain

$$f_1(x) = (x-\alpha) f_2(x), \text{ for some } f_2(x) \in \mathbb{F}[x],$$

And thus $f(x) = (x-\alpha)^2 f_2(x)$. In case $f_2(\alpha)=0$ we obtain a third factor $x-\alpha$. Continuing in this way we finally arrive at a factorization

$$f(x) = (x-\alpha)^k f_k(x), \quad f_k(\alpha) \neq 0.$$

We say that α is a root of multiplicity k. A root of multiplicity 1 is also called a simple root. By a multiple root we mean a root whose multiplicity is greater than 1.

Let us assume that $\beta \in \mathbb{F}$ is another root of $f(x)$ and let l denote the multiplicity of β. Then $f(\beta) = (\beta-\alpha)^k f_k(\beta) = 0$. Thus $f_k(\beta)=0$ since $(\beta-\alpha)^k \neq 0$. Therefore $(x-\beta)^l$ divides $f_k(x)$, i.e., $f_k(x) = (x-\beta)^l f_l(x)$ for some $f_l(x) \in \mathbb{F}[x]$, and

$$f(x) = (x-\alpha)^k (x-\beta)^l f_l(x)$$

If $f(x)$ has roots other than α and β, then we obtain more powers of linear factors that divides $f(x)$. Since $f(x)$ has finite degree, say n, the number of linear factors, each counted according to its multiplicity, cannot exceed n. This gives

Thm5 (D'Alembert's Theorem) Let $\mathbb{F}$ be a field and let f be a polynomial of degree $n \geq 1$ over $\mathbb{F}$. Then f has at most n roots in $\mathbb{F}$.

Example 1. Let $f(x) = -x^4+3x^2-4x-5$. Use the remainder theorem to find $f(-3)$

Solution: $f(x) = (x+3)(-x^3+3x^2-6x+14)+37$. Hence, $f(-3)=37$.